

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2004年11月18日 (18.11.2004)

PCT

(10) 国際公開番号  
WO 2004/099998 A1(51) 国際特許分類<sup>7</sup>: G06F 12/14, 15/00, 17/60

(21) 国際出願番号: PCT/JP2004/006042

(22) 国際出願日: 2004年4月27日 (27.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願2003-131005 2003年5月9日 (09.05.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 田口 大悟 (TAGUCHI, Daigo) [JP/JP]; 〒1088001 東京都港区芝

五丁目7番1号 日本電気株式会社内 Tokyo (JP). 堀 勇一 (KAWA, Yuichi) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP). 野田 潤 (NODA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP).

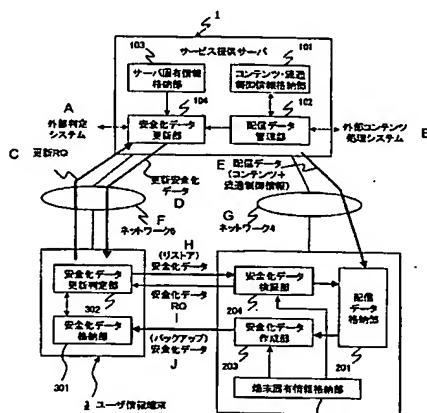
(74) 代理人: 速水 進治 (HAYAMI, Shinji); 〒1500021 東京都渋谷区恵比寿西2-17-16 代官山 T Kビル 1階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: DIGITAL INFORMATION DISTRIBUTION CONTROL METHOD AND DISTRIBUTION CONTROL SYSTEM

(54) 発明の名称: デジタル情報の流通制御方法および流通制御システム



1...SERVICE PROVIDING SERVER  
103...SERVER UNIQUE INFORMATION STORAGE SECTION  
101...CONTENT DISTRIBUTION CONTROL INFORMATION STORAGE SECTION  
A...EXTERNAL JUDGMENT SYSTEM  
104...SAFETY-GUARANTEERING DATA UPDATE SECTION  
102...DISTRIBUTION DATA MANAGEMENT SECTION  
B...EXTERNAL CONTENT PROCESSING SYSTEM  
C...UPDATED RQ  
D...UPDATED SAFETY-GUARANTEERING DATA  
E...DISTRIBUTION DATA (CONTENT + DISTRIBUTION CONTROL INFORMATION)  
F...NETWORK 5  
G...NETWORK 4  
302...SAFETY-GUARANTEERING DATA UPDATE JUDGEMENT SECTION  
301...SAFETY-GUARANTEERING DATA STORAGE SECTION  
H...(RESTORE) SAFETY-GUARANTEERING DATA  
I...SAFETY-GUARANTEERING DATA RQ  
J...(BACKUP) SAFETY-GUARANTEERING DATA  
3...USER INFORMATION TERMINAL  
204...SAFETY-GUARANTEERING DATA VERIFICATION SECTION  
203...SAFETY-GUARANTEERING DATA CREATION SECTION  
201...DISTRIBUTION DATA STORAGE SECTION  
202...TERMINAL UNIQUE INFORMATION STORAGE SECTION  
2...MOBILE INFORMATION TERMINAL

(57) Abstract: A server (1) generates distribution data consisting of content data such as a digital content and an electronic ticket to which distribution control information indicating the data transmission enabled/disabled state, the encryption required/not-required state, server enquiry enabled/disabled state, and the like is added and distributes it to a mobile information terminal (2). The distribution data is stored in the mobile information terminal (2) and freely used by a service user. The distribution data can be backed up in another user information terminal but its restoring or transmission is limited according to the distribution control information added.

(57) 要約: サーバ (1) は、デジタルコンテンツや電子チケットなどのコンテンツデータに、データ転送の可否、暗号化の可否、サーバ問合せの可否等を指示する流通制御情報を付加した配信データを生成し、携帯情報端末 (2) へ配信する。配信データは携帯情報端末 (2) に格納されてサービス利用者により自由に利用される。配信データは他のユーザ情報端末にバックアップ可能であるが、付加された流通制御情報に従ってリストアあるいは転送には制限を課される。



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

## 明 細 書

## デジタル情報の流通制御方法および流通制御システム

## 5 技術分野

本発明はデジタル情報への不正なアクセスを防止するためのデジタル情報管理技術に係り、特に提供されるサービスに対する不正アクセスの防止とサービス利用者の利便性とを考慮したデジタル情報流通制御システムおよび方法に関する。

10

## 背景技術

近年、デジタルコンテンツ配信サービスが普及し、アプリケーションソフト、音楽、映像、雑誌、チケットなどもネットワークを通して配信されるようになってきた。このようなコンテンツは著作物や商品であるから、どのよう

15 くに保護するかはますます重要な課題となっている。

たとえば、携帯電話機の着信メロディを配信するサービスでは、その著作権を保護する技術としてSMAF (Synthetic music Mobile Application Format)が主に採用されている。SMAFはヤマハ株式会社が設計したデータフォーマット仕様であり、主に携帯情報端末や携帯電話機で再生するマルチメディアコンテンツのデータ形式を定義するために用いられる。SMAFによれば、SMAFデータに(A)保存可・転送可、(B)保存可・転送不可、(C)保存不可・転送不可の3つのコピーステータス(C o p y S t a t u s)を設定することができる。したがって、コピーステータスに応じて、データの保存や他の携帯電話機への転送が可能／不可能となり、不正な

20 データ転送などを防止することができる。

25

このように携帯電話機にダウンロードしたコンテンツは、携帯電話機を交換したときあるいは操作ミスなどで消失したときのために、ユーザのパーソナルコンピュータなどにバックアップをとっておくことが望ましい。しかし

ながら、バックアップを無制限に認めることは正当な使用者以外の者に違法コピーされる可能性も有しているために、サービス提供者としては著作権保護も併せて考慮しなければならない。

特開 2 0 0 2 - 1 8 5 5 7 9 号公報（特許文献 1）には、このような著作権保護を考慮したバックアップ方法が開示されている。この従来の方法では、  
5 携帯電話機からパーソナルコンピュータへ J A V A（登録商標）アプリケーションをバックアップする際に携帯電話機の製造番号と電話番号とを付加し、復元する際に携帯電話機の製造番号および／または電話番号を比較することで、J A V A（登録商標）アプリケーションの不正使用を防止する。

10 また、データの改ざんの有無を検知するデジタル署名技術やデータの不正閲覧や盗聴を防止する暗号技術などを用いることでバックアップやリストア時のデータ保護を図ることも可能である。

特許文献 1 特開 2 0 0 2 - 1 8 5 5 7 9 号公報（段落番号 0 0 1 8 ～ 0 0 2 3、0 0 2 6 ～ 0 0 2 8、図 4）。

15

#### 発明の開示

しかしながら、上記従来のバックアップ方法にデジタル署名あるいは暗号化技術を組み合わせても、次のようなデータ不正使用を防止することはできない。たとえば、サービス利用者は残数 1 0 回の電子チケットをサービス提供者から受信し、携帯電話機に格納する。この電子チケットは、対応するサ  
20 ービスを享受する度に 1 回ずつ残数が減るような電子チケットである。サービス利用者は、上記従来のバックアップ方法により残数 1 0 回の電子チケットをパーソナルコンピュータへバックアップする。次に、携帯電話機を用いて通常の手順で 1 0 回のサービスを享受する。その後、バックアップデータ  
25 を携帯電話機に復元する。この場合、同じ携帯電話機であるから正常にリストアされる。したがって、この携帯電話機は、残数 1 0 回の電子チケットが正常にリストアされ、再びサービス利用可能状態となってしまう。

このように従来技術では、携帯情報端末や携帯電話機などの携帯通信機器

ヘデジタルコンテンツや電子チケットを配信するサービス事業者の権利保護とサービスを享受するサービス利用者の利便性とを十分に両立させることができなかった。

そこで、本発明の目的は、サービス提供者の権利保護とサービス利用者の  
5 利便性とを共に確保することができるデジタル情報の流通制御システムおよび方法を提供することにある。

また、本発明の他の目的は、配信されたデータのバックアップおよびリストアの正当性を確実に判定することができるデジタル情報の流通制御システムおよび方法を提供することにある。

10 さらに、本発明のその他の目的は、配信されたデータをバックアップおよびリストアするための条件を柔軟に設定できるデジタル情報の流通制御システムおよび方法を提供することにある。

本発明による流通制御方法は、デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末と、を有するシステムにおけるデジタル情報の流通制御方法であって、前記デジタル情報と  
15 データ転送制御条件を示す流通制御情報とを含む配信データを前記サーバから前記情報処理端末へ配信し、前記情報処理端末に前記配信データを格納し、前記流通制御情報に従って前記情報処理端末と他の情報処理端末との間での前記配信データを含む情報の転送を制御する、ことを特徴とする。

20 前記転送制御は、前記情報処理端末の固有情報を用いて生成された前記配信データを含む情報を前記他の情報処理端末へ転送して格納し、前記他の情報処理端末に格納された配信データを含む情報を前記情報処理端末へ再格納する前に、前記流通制御情報に従って前記情報処理端末への再格納の可否を判定する、ことを特徴とする。あるいは、前記転送制御は、前記情報処理  
25 端末の固有情報を用いて生成された前記配信データを含む情報を前記他の情報処理端末へ転送して格納し、前記他の情報処理端末に格納された配信データを含む情報を前記情報処理端末へ再格納する前に、前記流通制御情報に従って前記サーバへの問合せの可否を判定する、ことを特徴とする。

前記流通制御情報は、望ましくは、前記配信データを含む情報の転送可否決定条件および前記サーバへの問合せの可否決定条件のうち少なくとも1つを含む。

5 本発明の一実施形態によれば、デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末とを有するシステムにおけるデジタル情報の流通制御方法は、前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを前記サーバから前記情報処理端末へ配信し、前記情報処理端末に前記配信データを格納し、前記情報処理端末に割り当てられた端末固有情報を用いて前記配信データを含む第  
10 1 安全化データを生成して他の情報処理端末へ転送し、前記他の情報処理端末に格納された安全化データに含まれる配信データを前記情報処理端末へ再格納する前に、安全化データ送信要求を前記他の情報処理端末へ送信し、前記情報処理端末の端末固有情報と、前記安全化データ送信要求に対応する第  
2 安全化データに含まれる端末固有情報および流通制御情報とに基づいて、  
15 当該第2 安全化データに含まれる配信データを前記情報処理端末へ再格納可能か否かを判定し、再格納可能であるときに前記第2 安全化データに含まれる前記配信データを前記情報処理端末に格納する、ことを特徴とする。

本発明によれば、デジタル情報の配信サービスを行うサーバから前記デジタル情報の配信を受け、バックアップ用の他の情報処理端末との間でデータ  
20 転送可能な携帯情報端末において、データ転送を制限する条件を示す流通制御情報と前記デジタル情報とを含む配信データを前記サーバから受信し格納する配信データ格納手段と、当該携帯情報端末に割り当てられた端末固有情報を格納する端末固有情報格納手段と、前記配信データ格納手段から前記他の情報処理端末へ前記配信データを転送するために、前記端末固有情報を用  
25 いて前記配信データを含む第1 安全化データを生成し、前記他の情報処理端末へ送信する安全化データ生成手段と、前記他の情報処理端末から第2 安全化データを受信して当該第2 安全化データに含まれる配信データを前記配信データ格納手段へ再格納する前に、前記他の情報処理端末へデータ送信要求

を行うデータ送信要求生成手段と、前記データ送信要求の応答として前記他の情報処理端末から前記第2安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第2安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第2安全化データが再格納可能か否かを検証し、再格納可能であるときに前記第2安全化データに含まれる配信データを前記配信データ格納手段に格納する安全化データ検証手段と、を有することを特徴とする携帯情報端末が提供される。

本発明によれば、情報処理端末に対してデジタル情報の配信サービスを行うサーバにおいて、当該サーバに割り当てられたサーバ固有情報を格納するサーバ固有情報格納手段と、前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを生成して前記情報処理端末へ配信する配信データ管理手段と、前記情報処理端末の端末固有情報および要求された安全化データを含む安全化データ問合せを受信すると、当該安全化データ問合せに含まれる前記安全化データの更新可否を判定し、更新可能な場合に当該安全化データを更新して前記安全化データ問合せの応答として返送する安全化データ更新手段と、を有することを特徴とするサーバが提供される。

本発明によれば、データ転送を制限する条件を示す流通制御情報とデジタル情報とを含む配信データをサーバから受信する携帯情報端末と接続可能であり、前記携帯情報端末が受信した前記配信データをバックアップする情報処理装置であって、前記携帯情報端末に割り当てられた端末固有情報を用いて生成された前記配信データを含む第1安全化データを格納する安全化データ格納手段と、前記安全化データ格納手段に格納された第1安全化データに含まれる配信データを前記携帯情報端末へ再格納するための安全化データ送信要求を前記携帯情報端末から受信し、当該受信したデータ送信要求と前記安全化データ格納手段に格納された第1安全化データの端末固有情報および流通制御情報とに基づいて、当該格納された第1安全化データを第2安全化データとして前記携帯情報端末へ返送するか否かを判定する判定手段と、を有することを特徴とする情報処理装置が提供される。

本発明によれば、デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信を受ける第1情報処理端末と、前記第1情報処理端末との間でデータ転送可能な第2情報処理端末と、を少なくとも有する流通制御システムにおいて、前記サーバは、データ転送を制限する条件を示す流通制御情報

5 報を前記デジタル情報に付加した配信データを生成して前記第1情報処理端末へ送信する配信データ管理手段を少なくとも有し、前記第1情報処理端末は、前記配信データを格納する配信データ格納手段と、前記第1情報処理端末に割り当てられた端末固有情報を格納する端末固有情報格納手段と、前記配信データ格納手段から前記第2情報処理端末へ前記配信データを転送する

10 ために、前記端末固有情報を用いて前記配信データを含む第1安全化データを生成し、前記第2情報処理端末へ送信する安全化データ生成手段と、前記第2情報処理端末から第2安全化データを受信して当該第2安全化データに含まれる配信データを前記配信データ格納手段へ再格納するために、前記第2情報処理端末へデータ送信要求を行うデータ送信要求生成手段と、前記データ送信要求の応答として前記第2情報処理端末から前記第2安全化データを受信すると、前記端末固有情報を用いて当該第2安全化データが再格納可能か否かを検証し、再格納可能であるときに前記第2安全化データに含まれる配信データを前記配信データ格納手段に格納する安全化データ検証手段と、

15 を少なくとも有し、前記第2情報処理端末は、前記第1情報処理端末から転送された前記第1安全化データを格納する安全化データ格納手段と、前記データ送信要求と前記安全化データ格納手段に格納された安全化データの端末固有情報および流通制御情報とに基づいて、当該格納された安全化データを第2安全化データとして前記第1情報処理端末へ返送するか否かを判定する判定手段と、を少なくとも有することを特徴とする流通制御システムが提供

20 される。

25

本発明によれば、コンピュータに、情報処理端末に対してデジタル情報の配信サービスを行うサーバ機能を実現するためのサーバプログラムにおいて、前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信デ



ータを生成して前記情報処理端末へ配信するステップと、前記情報処理端末の端末固有情報および要求された安全化データを含む安全化データ問合せを受信すると、当該安全化データ問合せに含まれる前記安全化データの更新可否を判定するステップと、更新可能な場合に当該安全化データを更新して前記安全化データ問合せの応答として返送するステップと、を有することを特徴とするサーバプログラムが提供される。

本発明によれば、コンピュータに、デジタル情報の配信サービスを行うサーバから前記デジタル情報の配信を受けると共にバックアップ用の他の情報処理端末との間でデータ転送を実行させる携帯情報端末用のプログラムにおいて、データ転送を制限する条件を示す流通制御情報と前記デジタル情報とを含む配信データを前記サーバから受信し格納するステップと、前記他の情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第1安全化データを生成し、前記他の情報処理端末へ送信するステップと、前記他の情報処理端末から第2安全化データを受信して当該第2安全化データに含まれる配信データを前記配信データ格納手段へ再格納する前に、前記他の情報処理端末へデータ送信要求を行うステップと、前記データ送信要求の応答として前記他の情報処理端末から前記第2安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第2安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第2安全化データが再格納可能か否かを検証するステップと、再格納可能であるときに前記第2安全化データに含まれる配信データを格納するステップと、を有することを特徴とする携帯情報端末用のプログラムが提供される。

上述したように、本発明によれば、情報処理端末に格納される配信データは、データ転送を制限する条件を示す流通制御情報をデジタル情報（デジタルコンテンツや電子チケットなどのコンテンツデータ）に付加したものである。流通制御情報としては、たとえば、データ転送の可否決定条件やサーバ問合せの可否決定条件が含まれる。これら条件は、フラグによる記述やプログラムのような手続き的な記述により設定することができる。配信データに

含まれるデジタル情報は情報処理端末に格納されてサービス利用者により自由に利用されるが、付加された流通制御情報により当該デジタル情報の転送はサービス提供者の権利が保護されるように制限することができる。これにより、配信データサービス提供者の権利保護とサービス利用者の利便性とを共に確保することができる。

また、他の情報処理端末にバックアップされた安全化データに含まれる配信データをリストアする場合、上述した流通制御情報により、リストアの禁止、無条件リストア許可、および、サーバ問合せのいずれかに設定することができる。サーバ問合せの場合では、サーバは、情報処理端末へリストアする正当性および安全化データの更新の可否を判定し、更新可能であれば、更新された安全化データを返す。これにより、バックアップおよびリストアの正当性を確実に判定することができる。また、流通制御情報の設定によりサーバに問い合わせる回数を少なくできるために、ネットワークおよびサーバの負荷を軽減できる。

以上詳細に説明したように、本発明によれば、サービス提供者がコンテンツデータに流通制御情報を付加して配信することにより、コンテンツデータの流通を制御することができる。たとえば、流通制御情報の設定により、サーバへの更新判定問い合わせ、あるいは、更新なしの安全化データリストアを選択することができ、ネットワークおよびサーバの負荷の増大を抑制できる。さらに、流通制御情報を用いることで、配信データのバックアップおよびリストアの正当性を確実に判定することができ、利用者の利益とサービス提供者の利益とを両立させることができる。特に、デジタル署名および暗号化技術を用いてデータ転送および検証を行うことで、より確かな正当性判定およびデータ保護が可能となる。また、流通制御情報の設定によりデータ転送が制御可能であるから、バックアップおよびリストアするための条件を柔軟に設定できる。

また、携帯情報端末へリストアされるコンテンツデータ（たとえば電子チケット）がサービス提供者サーバで管理するコンテンツデータと一致するこ

とを保証する流通制御情報を設定し、携帯情報端末に格納されているコンテンツデータが正しいことを保証できる。このため、コンテンツデータをチェックしてデジタル情報や物品の提供／貸与管理、乗車／乗船などの入場管理を実施する際に、サービス提供者サーバに問い合わせることなく、コンテンツデータを信頼して提供／貸与、入場管理を行うことができる。紛失などに伴うリストア操作は、通常のコンテンツデータ利用操作に比べ、圧倒的にその回数が少ないと考えられるため、サービス提供者が運営する電子チケットサーバの負荷を大幅に軽減することができる。

さらに、システム管理者は、サービス提供者へサービス提供者IDやサービス提供者証明書を発行し、携帯情報端末へ端末識別情報やユーザID、端末証明書などを発行、格納する処理を、サービス提供者がサービスを立ち上げるとき、及び、サービス利用者が新たな携帯情報端末の利用を開始するときに実施すればよい。したがって、サービス利用者がデジタルコンテンツや電子チケットのバックアップやリストアを実行する度に実施すべき処理はない。このため、多数のサービス提供者、多数の携帯情報端末が存在し、膨大なデジタルコンテンツや電子チケットが流通する環境においても、システム管理者が実施する処理はサービス提供者数と携帯情報端末数に比例しており、スケーラビリティに優れたデジタル情報流通制御を実現することができる。

また、ユーザ情報端末へバックアップしたデジタルコンテンツや電子チケットは、必要に応じて暗号化されており、ユーザ情報端末における閲覧や不正コピーを防止できる。また、ユーザ情報端末において改ざんしたデータは携帯情報端末へリストアできないため、サービス提供者は安心して、サービス利用者にデジタルコンテンツや電子チケットのバックアップとリストアを許可することが可能になる。このためサービス利用者は、携帯情報端末の紛失に備えたバックアップやリストアが可能となり、利便性が向上する。

#### 図面の簡単な説明

上述した目的、およびその他の目的、特徴および利点は、以下に述べる好

適な実施形態、およびそれに付随する以下の図面によってさらに明らかになる。

図 1 は、本発明の第 1 実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。

- 5 図 2 は、図 1 のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。

図 3 は、図 1 に示すデジタル情報流通制御システムのより詳細な機能構成を示すブロック図である。

- 10 図 4 は、携帯情報端末 2 の端末固有情報格納部 2 0 2 に格納される端末固有情報を示す模式図である。

図 5 は、サービス提供者サーバ 1 のサーバ固有情報格納部 1 0 3 に格納されるサーバ固有情報を示す模式図である。

- 15 図 6 は、(A) は配信データ生成部 2 1 0 3 で生成される配信データの構成の一例を示す模式図であり、(B) はその流通制御情報の記述例を示す模式図である。

- 20 図 7 は、(A) は、安全化データ生成部 2 2 0 3 で生成され、送信時にコンテンツボディの暗号化を行わないと指定されたバックアップ用安全化データの構成例を示す模式図であり、(B) は、安全化データ生成部 2 2 0 3 で生成され、送信時にコンテンツボディの暗号化を行うと指定されたバックアップ用安全化データの構成例を示す模式図である。

図 8 は、安全化データリクエスト生成部 2 2 0 4 で生成する安全化データリクエストの構成例を示す模式図である。

図 9 は、更新要否判定部 2 3 0 3 の安全化データ更新判定動作の一例を示すフローチャートである。

- 25 図 1 0 は、更新リクエストの構成例を示す模式図である。

図 1 1 は、(A) は、安全化データ更改部 2 1 0 9 で生成され、送信時にコンテンツボディの暗号化を行わないと指定された更新安全化データの構成例を示す模式図であり、(B) は、安全化データ更改部 2 1 0 9 で生成され、

送信時にコンテンツボディの暗号化を行うと指定された更新安全化データの構成例を示す模式図である。

図 1 2 は、データ安全性確認部 2 2 0 6 におけるデータ安全性確認動作の一例を示すフローチャートである。

- 5 図 1 3 は、本発明の第 1 実施形態によるデジタル情報流通制御システムの第 1 の適用例を示す概略的システム機能図である。

図 1 4 は、第 1 実施形態におけるサービス提供者サーバ 1 の他の例を示す概略的ブロック図である。

- 10 図 1 5 は、第 1 実施形態における携帯情報端末 2 およびユーザ情報端末 3 の他の例を示す概略的ブロック図である。

図 1 6 は、本発明の第 2 実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。

図 1 7 は、本発明の第 2 実施形態によるデジタル情報流通制御システムの適用例を示す概略的システム機能図である。

- 15 図 1 8 は、本発明の第 3 実施形態によるデジタル情報流通制御システムを示す概略的システム機能図である。

図 1 9 は、図 1 8 のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。

- 20 図 2 0 は、有効期限情報を含む更新安全化データを受信したときのデータ安全性確認部 2 2 0 6 のデータ安全性確認動作の一例を示すフローチャートである。

図 2 1 は、本発明の第 5 実施形態における安全化データリクエストの構成例を示す模式図である。

- 25 図 2 2 は、乱数  $r$  を含む更新安全化データを受信したときのデータ安全性確認部 2 2 0 6 のデータ安全性確認動作の一例を示すフローチャートである。

図 2 3 は、本発明の第 6 実施形態における流通制御情報の一例を示す模式図である。

発明を実施するための最良の形態

## 1. 第1実施形態

図1は、本発明の第1実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。本実施形態によるシステムは、サービス提供者サーバ1、通信機能を有する携帯情報端末2、および通信機能を有するユーザ情報端末3を含み、サービス提供者サーバ1と携帯情報端末2およびユーザ情報端末3とがネットワーク4および5によりそれぞれ接続可能であるものとする。

### (1) システム構成のアウトライン

サービス提供者サーバ1は、デジタルコンテンツや電子チケットなどのコンテンツデータに流通制御情報を付加し、配信データとしてネットワーク4を通して携帯情報端末2へ送信する。さらに、後述するように、ユーザ情報端末3からの問い合わせに対して更新されたデータを送信する機能も有する。

携帯情報端末2はサービス提供者サーバ1から受信した配信データを格納する。携帯情報端末2はサービス利用者が所有する携帯通信端末や携帯電話機などであり、サービス利用者は、たとえば所定のサービスポイントで電子チケット（入場券など）を利用することができる。さらに、後述するように、携帯情報端末2は配信データのバックアップおよびリストア機能も有する。

ユーザ情報端末3は、ケーブルあるいはワイヤレスにより携帯情報端末2と接続可能であり、携帯情報端末2に格納された配信データのバックアップおよびリストアを行うことができる。後述するように、バックアップされた配信データを携帯情報端末2へリストアする時には、所定の条件に従ってサービス提供者サーバ1へ問い合わせることができる。ユーザ情報端末3としては、ネットワーク5を通してサービス提供者サーバ1に接続可能な通信機能を有するパーソナルコンピュータが典型例であるが、その他ネットワーク5に接続されたバックアップ用のコンピュータであってもよい。

図1を参照して更に詳しく説明すると、サービス提供者サーバ1は、コンテンツ・流通制御情報格納部101、配信データ管理部102、サーバ固有

情報格納部 1 0 3 および安全化データ更新部 1 0 4 を含む。コンテンツ・流通制御情報格納部 1 0 1 はデジタルコンテンツや電子チケットなどのコンテンツデータと流通制御情報とを格納する。

5 流通制御情報は、配信データの流通を制御する情報であり、詳しくは後述するが、携帯情報端末 2 およびユーザ情報端末 3 間でのデータ転送の可否、データ転送時の暗号化の要否、あるいは、サービス提供者サーバ 1 への更新問合せの可否などの少なくとも 1 つまたは複数について指示する情報である。また、この流通制御情報は、制御フラグまたは手続的記述などにより表現可能である。

10 配信データ管理部 1 0 2 は、コンテンツ・流通制御情報格納部 1 0 1 に格納されているコンテンツデータおよび流通制御情報を管理し、それらから生成された配信データを携帯情報端末 2 へ配信し、あるいは安全化データ更新部 1 0 4 へ出力する。なお、コンテンツデータの管理は、外部コンテンツ処理システムと連携して行われる場合もある。たとえば、コンテンツデータが  
15 電子チケットの場合には、サービス利用者がサービスを利用する毎に更新される。したがって、その更新内容をコンテンツ・流通制御情報格納部 1 0 1 に格納されているコンテンツデータに反映させる必要がある。この場合には、配信データ管理部 1 0 2 はネットワーク等を通して外部コンテンツ処理システムに接続されている。

20 サーバ固有情報格納部 1 0 3 は、サービス提供者サーバ 1 に割り当てられた識別情報やデジタル署名作成および検証のための情報などを含むサーバ固有情報を格納する。

安全化データ更新部 1 0 4 は、ユーザ情報端末 3 から受信した安全化データ更新リクエストに応じた安全化データ更新の可否を判定し、更新可能な場合  
25 には安全化データの更新を実行する。なお、安全化データ更新リクエストに応じた安全化データ更新の可否判定は、外部判定システムと連携して行われる。

外部判定システムは、例えば紛失や老朽化などの事由によって携帯情報端

末 2 が機種変更された場合、その変更に伴う端末識別情報などの変更を登録しておき、更新リクエストのコンテンツデータが携帯情報端末 2 が変更された後でも再発行可能であるか否かを判定する。更新リクエストの端末識別情報が端末変更起因するものであれば、再発行可能なコンテンツデータであり更新可能であると判定する。更新リクエストの端末識別情報が端末変更と何ら関係がない場合には、更新不可能と判定する。なお、外部判定システムの判定方法は、これに限定されるものではなく、更新リクエストに含まれる情報を利用する他の判定方法でもかまわない。

携帯情報端末 2 は、配信データ格納部 201、端末固有情報格納部 202、安全化データ作成部 203 および安全化データ検証部 204 を有する。配信データ格納部 201 は、サービス提供者サーバ 1 から受信した配信データあるいは安全化データ検証部 204 から入力したバックアップされた配信データをリストアする。

端末固有情報格納部 202 は、携帯情報端末 2 に割り当てられた端末識別情報、デジタル署名作成および検証のための情報、コンテンツ暗号化鍵やその証明書情報およびコンテンツ復号化鍵などを含む端末固有情報を格納する。

安全化データ作成部 203 は、配信データ格納部 201 に格納されている配信データと端末固有情報格納部 202 に格納されている端末固有情報とを利用してバックアップ用の安全化データを作成し、ユーザ情報端末 3 へ送信する。安全化データは、後述するように、そこに含まれるコンテンツデータの不正閲覧を防止でき、かつ、改ざんの有無を検知することができる。

安全化データ検証部 204 は、バックアップデータのリストアをしようとする時、ユーザ情報端末 3 へバックアップした安全化データの送信を要求する（安全化データリクエスト）。その要求に応じたユーザ情報端末 3 から安全化データを受信すると、受信した安全化データに含まれる配信データが保存可能か否かを検証する。保存可能である場合には、受信した配信データを配信データ格納部 201 に格納する。

ユーザ情報端末 3 は安全化データ格納部 301 および安全化データ更新判



定部 3 0 2 を有する。安全化データ格納部 3 0 1 は、携帯情報端末 2 から受信したバックアップ用の安全化データを格納する。

安全化データ更新判定部 3 0 2 は、携帯情報端末 2 からの要求に応じて、安全化データ格納部 3 0 1 に保存されたバックアップ安全化データに含まれる識別情報や流通制御情報をチェックし、当該安全化データが更新を必要とするか否かを判定する。更新が不要である場合には、携帯情報端末 2 へ当該安全化データをリストア用の安全化データとして送信する。更新が必要で、かつ、サーバ問合せによる安全化データの更新が許可されている場合には、サービス提供者サーバ 1 へ当該安全化データを送信して更新を依頼し、サービス提供者サーバ 1 で更新された安全化データを受信する。そして、サービス提供者サーバ 1 から受信した安全化データをリストア用の安全化データとして携帯情報端末 2 へ送信する。

図 2 は、図 1 のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。

上述したように、本実施形態によるデジタル情報流通制御システムでは、コンテンツデータに流通制御情報が付加された配信データがサービス提供者サーバ 1 から携帯情報端末 2 へ配信され、流通制御情報によりデータ転送の可否、データ転送時の暗号化の要否、サービス提供者サーバ 1 への更新問合せの可否などが指示される。

図 2 に示すように、受信した配信データは携帯情報端末 2 の配信データ格納部 2 0 1 に保存され利用に供される。配信データをバックアップする時には、配信データを配信データ格納部 2 0 1 から読み出し、端末固有情報格納部 2 0 2 に格納された端末固有情報を用いて改ざん等を検知できる安全化データを作成する（ステップ S 0 1）。この安全化データをユーザ情報端末 3 へ送信し、ユーザ情報端末 3 の安全化データ格納部 3 0 1 に格納する（ステップ S 0 2）。

バックアップされた配信データをリストアする時には、携帯情報端末 2 から安全化データリクエストをユーザ情報端末 3 へ送信する。安全化データ更

新判定部 3 0 2 は、安全化データリクエストの識別情報とバックアップ安全化データの識別情報および流通制御情報とを用いて、バックアップ安全化データをそのまま返信できるか否か、それともサービス提供者サーバ 1 への問い合わせが必要か否か、をデータ転送前に判断する（ステップ S 0 3）。問い合わせが必要であれば、バックアップ安全化データおよび安全化データリクエストから更新リクエストを生成してサービス提供者サーバ 1 へ送信する（ステップ S 0 4）。

サービス提供者サーバ 1 は、更新リクエストを受信すると、当該安全化データに含まれるコンテンツデータが改ざんされていない正しい情報であるか否かおよび外部判定システムと連携して更新の可否を判定する（ステップ S 0 5）。正しい情報でありかつ更新可と判定されれば、配信データ管理部 1 0 2 から最新の配信データを読み出し、更新された安全化データを生成してユーザ情報端末 3 へ返信する（ステップ S 0 6）。なお、サービス提供者は、流通制御情報として予めリストア条件を設定することができるが、コンテンツデータ配信後に利用者が携帯情報端末 2 の機種変更をしたり、家族が新規に家族割引で契約したりしてもその情報を流通制御情報として与えることはできない。このため、サービス提供者サーバ 1 にとっても、コンテンツ配信後の携帯情報端末 2 の機種変更や家族割引契約情報などは未知の情報である。したがって、機種変更や家族割引契約などに応じてデータ更新可否を制御するためには外部判定システムとの連携が必要である。

サービス提供者サーバ 1 から更新リクエストに対する更新安全化データを受信すると、安全化データ更新判定部 3 0 2 はそれをリストア用の安全化データとして携帯情報端末 2 へ送信する。また、安全化データ格納部 3 0 1 から読み出した安全化データがサーバ問合せを必要としないデータであれば、安全化データ更新判定部 3 0 2 はそれをそのままリストア用の安全化データとして携帯情報端末 2 へ送信する（ステップ S 0 3）。

こうして安全化データリクエストの応答としてユーザ情報端末 3 から安全化データを受信すると、携帯情報端末 2 の安全化データ検証部 2 0 4 は、端

- 末固有情報を参照しながら、受信した安全化データが改ざんされていない正しい情報であるか否か、および、配信データ格納部 201 に格納して良いか否かを判定する（ステップ S07）。正しい情報でかつ格納許可された安全化データの配信データのみが配信データ格納部 201 に格納され、配信データのリストアが完了する。

- 上述した動作により、配信データのバックアップおよびリストアの正当性を確実に判定することができ、利用者の利益とサービス提供者の利益とを両立させることができる。特に、次に説明するようにデジタル署名および暗号化技術を用いてデータ転送および検証を行うことで、より確かな正当性判定およびデータ保護が可能となる。また、流通制御情報の設定によりデータ転送が制御可能であるから、バックアップおよびリストアするための条件を柔軟に設定できる。さらに、流通制御情報の設定により、サーバ 1 への更新判定問い合わせ、および、更新なしの安全化データリストアを選択することができ、ネットワークおよびサーバの負荷を不必要に増大させることを回避できる。

以下、デジタル情報流通制御システムの具体例を用いて、本実施形態の構成および動作を更に詳細に説明する。

## （２）システムの機能構成

- 図 3 は、図 1 に示すデジタル情報流通制御システムのより詳細な機能構成を示すブロック図である。また、図 4 は携帯情報端末 2 の端末固有情報格納部 202 に格納される端末固有情報を示す模式図であり、図 5 はサービス提供者サーバ 1 のサーバ固有情報格納部 103 に格納されるサーバ固有情報を示す模式図である。

### 携帯情報端末

- 配信データ格納部 201 は、サービス提供者サーバ 1 から配信データを受信する配信データ受信部 2201 と、受信した配信データを記憶する配信データメモリ 2202 と、を有している。

端末固有情報格納部 202 は、図 4 に示すように、携帯情報端末 2 とユー

- ザ情報端末 3 との間を流通する情報に付与するデジタル署名を作成する流通署名作成鍵  $s_k t$  と、付与されたデジタル署名を検証する流通署名検証鍵  $v_k t$  と、流通署名検証鍵  $v_k t$  に対するデジタル証明書である端末証明書  $c\_v_k t$  と、コンテンツデータを暗号化するためのコンテンツ暗号化鍵  $e_k$  と、コンテンツ暗号化鍵  $e_k$  に対応するコンテンツ復号鍵  $d_k$  と、コンテンツ暗号化鍵  $e_k$  に対するデジタル証明書であるコンテンツ暗号化鍵証明書  $c\_e_k$  と、携帯情報端末あるいは携帯情報端末の所有者を識別するための ID 情報と、を格納している。ID 情報は、たとえば、携帯情報端末毎にユニークに割り当てられた端末識別情報  $ID_t$ 、所有者毎にユニークに割り当てられた所有者識別情報  $ID_u$  などである。ただし、ID 情報はこれらに限定されるものではなく、たとえば携帯情報端末や所有者をグループに分類するためのグループ ID や家族 ID などを含んでもよい。なお、本実施形態における ID 情報は、端末識別情報  $ID_t$  と所有者識別情報  $ID_u$  とからなるものとする。
- 15 安全化データ作成部 203 は、安全化データ生成部 2203 を有する。安全化データ生成部 2203 は、端末識別情報  $ID_t$ 、所有者識別情報  $ID_u$ 、配信データ、流通署名  $S_1$ 、流通署名検証鍵  $v_k t$ 、および端末証明書  $c\_v_k t$  を含む安全化データを生成する。ここで、流通署名  $S_1$  は、配信データと端末識別情報  $ID_t$  および所有者識別情報  $ID_u$  とを含む情報に対して
- 20 流通署名作成鍵  $s_k t$  を用いたデジタル署名処理を実行することにより生成される。なお、後述するように、配信データに含まれるコンテンツデータをコンテンツ暗号化鍵  $e_k$  を用いて暗号化したものを用いて、安全化データを生成してもよい。こうして生成された安全化データは、送受信部 2207 を通してユーザ情報端末 3 へ送信される。
- 25 安全化データ検証部 204 は、安全化データリクエスト生成部 2204 と、流通署名検証鍵検証部 2205 およびデータ安全性確認部 2206 と、を有する。

安全化データリクエスト生成部 2204 は、ユーザ情報端末 3 に保存され

ている安全化データを要求するために、端末識別情報 I D t および所有者識別情報 I D u を含む安全化データリクエスト、あるいは、端末識別情報 I D t、所有者識別情報 I D u、コンテンツ暗号化鍵 e k およびコンテンツ暗号化鍵証明書 c \_ e k を含む安全化データリクエストを生成する。生成された安全化データリクエストは送受信部 2 2 0 7 を通してユーザ情報端末 3 へ送信される。

安全化データリクエストの応答として安全化データが送受信部 2 2 0 7 を通してユーザ情報端末 3 から受信されると、その安全化データは、サービス提供者サーバ 1 で更新されたものか、あるいは、携帯情報端末 2 で生成されユーザ情報端末 3 にバックアップされたもののいずれかである。

流通署名検証鍵検証部 2 2 0 5 は、受信した安全化データに含まれる端末証明書 c \_ v k t あるいはサービス提供者証明書 c \_ v k s (図 5 参照) を利用して、当該安全化データに含まれる流通署名検証鍵 v k t あるいは v k s が正しいことを検証する。

データ安全性確認部 2 2 0 6 は、流通署名検証鍵が検証された安全化データに付与されている流通署名を利用して、当該安全化データが改ざんされていない正しいデータであることを確認すると共に、当該安全化データが携帯情報端末 2 で生成したものか、サービス提供者サーバ 1 で生成されたものを判定する。さらに、当該安全化データに含まれる配信データを配信データメモリ 2 2 0 2 へ保存してよいか否かを判定する。保存可能と判定された場合には配信データメモリ 2 2 0 2 へ保存する。もし安全化データに含まれるコンテンツデータが暗号化されていれば、コンテンツ復号鍵によって復号してから保存する。

ユーザ情報端末

ユーザ情報端末 3 は携帯情報端末 2 との間でデータのやりとりを行うための送受信部 2 3 0 1 を有し、安全化データ格納部 3 0 1 は受信した安全化データを記憶する安全化データメモリ 2 3 0 2 を有する。

安全化データ更新判定部 3 0 2 は、更新要否判定部 2 3 0 3、更新リクエ

スト生成部 2304、および、送受信部 2305 を有する。

- 送受信部 2301 により携帯情報端末 2 から安全化データリクエストを受信すると、更新要否判定部 2303 は、安全化データメモリ 2302 に記憶されているバックアップ安全化データに含まれる流通制御情報と、受信した
- 5 安全化データリクエストに含まれる端末識別情報 ID t あるいは所有者識別情報 ID u とを比較し、当該バックアップ安全化データの更新の要否を判定する。

- 更新要否判定部 2303 によって更新不要と判定された場合には、当該バックアップ安全化データは送受信部 2301 を通してそのまま携帯情報端末
- 10 2 へ送信される。更新要否判定部 2303 により更新が必要と判定された場合には、更新リクエスト生成部 2304 はバックアップ安全化データと安全化データリクエストとを含む更新リクエストを生成し、送受信部 2305 を通してサービス提供者サーバ 1 へ送信する。

- この更新リクエストに対する応答として、サービス提供者サーバ 1 から更
- 15 新済みの安全化データを送受信部 2305 で受信すると、当該更新済み安全化データは送受信部 2301 を通して携帯情報端末 2 へ送信される。更新済み安全化データを受信した携帯情報端末 2 では、上述したように、流通署名検証鍵検証部 2205 およびデータ安全性確認部 2206 により更新済み安全化データの正当性および安全性が確認された後、配信データメモリ 220
- 20 2 に格納される。

サービス提供者サーバ

- コンテンツ／流通制御情報格納部 101 は、サービス利用者に配信するデジタルコンテンツや電子チケット等のコンテンツデータを記憶するコンテンツメモリ 2101 と、コンテンツデータの各々に対応する流通制御情報を記
- 25 憶する流通制御情報メモリ 2102 とを含む。なお、上述したように、コンテンツメモリ 2101 のコンテンツデータによっては、外部コンテンツ処理システム 2401 によりその内容が更新されるものもある。

配信データ管理部 102 は、コンテンツメモリ 2101 に記憶されている

コンテンツデータとそれに対応する流通制御情報とから配信データを生成する配信データ生成部 2 1 0 3 と、配信データを携帯情報端末 2 へ配信する配信データ配信部 2 1 0 4 とを有している。

サーバ固有情報格納部 1 0 3 は、図 5 に示すように、サービス提供者の識別情報 I D s と、携帯情報端末 2、ユーザ情報端末 3 およびサービス提供者サーバ 1 の間を流通する情報に付与するデジタル署名を作成するための流通署名作成鍵 s k s と、付与されたデジタル署名を検証するための流通署名検証鍵 v k s と、流通署名検証鍵に対するデジタル証明書であるサービス提供者証明書 c \_ v k s と、を格納している。

10 安全化データ更新部 1 0 4 は、送受信部 2 1 0 5、流通署名検証鍵検証部 2 1 0 6、更新可否判定部 2 1 0 7、コンテンツ暗号化鍵検証部 2 1 0 8、および、安全化データ更改部 2 1 0 9 を有する。

送受信部 2 1 0 5 によりユーザ情報端末 3 から更新リクエストを受信すると、流通署名検証鍵検証部 2 1 0 6 は、更新リクエストに含まれる端末証明書 c \_ v k t を利用して当該更新リクエストに含まれる流通署名検証鍵 v k t が正しいことを検証する。続いて、更新可否判定部 2 1 0 7 は、検証された流通署名検証鍵を用いて、当該更新リクエストに含まれる安全化データが改ざんされていない正しい情報であることを検証し、さらに、外部判定システム 2 4 0 2 においてサービス提供者が決定する更新要件を参照し、更新リクエストに含まれる安全化データの更新可否を判定する。更新可能であれば、コンテンツ暗号化鍵検証部 2 1 0 8 は、更新リクエストに含まれるコンテンツ暗号化鍵証明書 c \_ e k を用いて更新リクエストに含まれるコンテンツ暗号化鍵 e k が正しいことを検証する。

コンテンツ暗号化鍵 e k の正当性が検証されると、安全化データ更改部 2 1 0 9 は、更新リクエストに含まれる安全化データを参照して、配信データ生成部 2 1 0 3 から対応する配信データを取得し、サーバ固有情報格納部 1 0 3 に格納されているサービス提供者識別情報 I D s、流通署名作成鍵 s k s、流通署名検証鍵 v k s およびサービス提供者証明書 c \_ v k s を用いて

更新安全化データを生成する。その際、正しいことが確認されたコンテンツ暗号化鍵  $e_k$  を用いてコンテンツデータを暗号化して更新安全化データを生成してもよい。こうして得られた更新安全化データは、更新リクエストの応答として、送受信部 2105 を通してユーザ情報端末 3 へ返信される。

5        (3) 動作例

まず、本発明によるデジタル情報流通制御システムでは、システム管理者がサービス提供者に対して

●サービス提供者サーバ毎に異なるサービス提供者識別情報の割り当ておよび発行

10      ●サービス提供者証明書の発行  
を実施する。

サービス提供者は、発行されたサービス提供者識別情報およびサービス提供者証明書、サービス提供者自身が作成したデータであることを証明するデジタル署名を作成するための流通署名作成鍵、および流通署名作成鍵に対応する流通署名検証鍵を管理する。特に流通署名作成鍵は他者に知られることのないように安全に管理する。ここで、流通署名作成鍵および流通署名検証鍵の作成は、サービス提供者によって実施されてもよく、この場合、システム管理者は、サービス提供者が示した流通署名検証鍵に対するサービス提供者証明書を発行すればよい。

20      また、システム管理者は、サービス利用者が所有する携帯情報端末 2 に対して、

●携帯情報端末毎に異なる端末識別情報の割り当ておよび各携帯情報端末への転送

●サービス利用者毎に異なる所有者識別情報の割り当ておよび各携帯情報  
25      端末への転送

●流通署名作成鍵およびそれに対応する流通署名検証鍵の作成と各携帯情報  
端末への転送

●端末証明書の作成および各携帯情報端末への転送



●コンテンツ暗号化鍵の各携帯情報端末への転送

●コンテンツ暗号化鍵に対応するコンテンツ復号鍵の生成および各携帯情報端末への転送  
を実施する。

- 5 特に、流通署名作成鍵およびコンテンツ復号鍵は携帯情報端末内の耐タンパ性(tamper-resistant)のあるストレージなどに格納し、悪意のユーザによる入手を困難にしておく。ここで、コンテンツ暗号化鍵は、システム管理者が作成して発行し携帯情報端末へ転送してもよいし、サービス利用者によって作成され、システム管理者に示したものを携帯情報端末へ転送してもよい。
- 10

また、コンテンツ暗号化鍵／コンテンツ復号鍵は公開鍵暗号系の暗号化鍵／復号鍵のペアであり、コンテンツ暗号化鍵で暗号化した情報は、対応するコンテンツ復号鍵でのみ復号でき、コンテンツ暗号鍵からコンテンツ復号化鍵を生成するための落とし戸関数を知らなければコンテンツ暗号化鍵からコンテンツ復号鍵を生成することは十分に困難であるものとする。尚、落とし戸関数はシステム管理者により十分安全に管理されているものとする。

15

次に、携帯情報端末2の端末固有情報格納部202は図4に示す端末固有情報を格納し、サービス提供者サーバ1のサーバ固有情報格納部103は図5に示すサーバ固有情報を格納しているものとし、本実施形態におけるデータ配信、バックアップおよびリストア動作の具体例を詳細に説明する。

20

#### データ配信

図6(A)は配信データ生成部2103で生成される配信データの構成の一例を示す模式図であり、(B)はその流通制御情報の記述例を示す模式図である。

- 25 図6(A)に示すように、配信データは管理用ヘッダ(H)、コンテンツボディ(B)および流通制御情報(P)から構成される。管理用ヘッダ

(H)は携帯情報端末2へ配信するコンテンツデータを個別に管理するための情報であり、サービス提供者名やコンテンツデータのシリアル番号などを

含んでいる。コンテンツボディ（B）は携帯情報端末 2 へ配信するデジタルコンテンツや電子チケットなどのコンテンツデータそのものである。

流通制御情報（P）は携帯情報端末 2 へ配信した配信データの流通を制御する情報である。たとえば、流通制御情報を含むデータを格納した情報端末からバックアップ用情報端末へデータを転送して格納しているものとする。そのバックアップデータをバックアップ用情報端末からある情報端末へリストアする際に、リストアを要求している情報端末とバックアップデータが示す情報端末との同一性、および、バックアップデータに含まれる流通制御情報が示す条件に基づいて、転送許可／サーバ問い合わせ／転送禁止が決定される。例えば、

- ・ 「バックアップしたデータに含まれる端末識別情報と、リストア先の情報端末が持つ端末識別情報とが一致した場合にはリストア許可」、
  - ・ 「バックアップしたデータに含まれる所有者識別情報と、リストア先の情報端末が持つ所有者識別情報とが一致しない場合には、サービス提供者サーバ 1 へ問合せ、その後リストア許可」、
  - ・ 「バックアップしたデータに含まれる端末識別情報と、リストア先の情報端末が持つ端末識別情報とが一致しない場合にはリストア不許可」
- のような制御が可能となる。

図 6（B）に示すように、ここでは、4つのフラグで記述された流通制御情報が一例として示されている。最初のフラグは同一端末間移動フラグ  $F_t$  で、禁止／許可／サービス提供者サーバ問合せの 3 値をとる。次のフラグは同一所有者間移動フラグ  $F_{u1}$  で、禁止／許可／サービス提供者サーバ問合せの 3 値をとる。次のフラグは異所有者間移動フラグ  $F_{u2}$  で、禁止／許可／サービス提供者サーバ問合せの 3 値をとる。次のフラグは暗号化フラグ  $F_{en}$  でコンテンツボディの暗号化を行わない／行うの 2 値をとる。

図 6（B）に示した例は流通制御情報の一例であり、それぞれのフラグは異なる順番でもよい。また、流通制御情報内に、端末識別情報や所有者識別情報を固定的に埋め込んでおき、埋め込まれた端末識別情報や所有者識別情

報と、安全化データの転送を要求する携帯情報端末 2 の端末識別情報や所有者識別情報との一致／不一致を条件として記述してもよい。さらに、端末識別情報や所有者識別情報が番号として記述される場合には、その大小関係を条件としてもよい。あるいは、後述するように、流通制御情報（P）をプログラムで手続き的に記述してもよい（図 2 3 参照）。

なお、配信データの管理用ヘッダおよびコンテンツボディはコンテンツメモリ 2 1 0 1 に記憶されており、流通制御情報は流通制御情報メモリ 2 1 0 2 に記憶されている。

配信データ生成部 2 1 0 3 で生成された配信データは、配信データ配信部 2 1 0 4 から携帯情報端末 2 へ配信され、携帯情報端末 2 において配信データ受信部 2 2 0 1 で受信されて配信データメモリ 2 2 0 2 に格納される。格納された配信データは、配信データ生成部 2 1 0 3 で生成した配信データと同様であり、図 6 に示す情報を含んでいる。

ここで、配信データ配信部 2 1 0 4 と配信データ受信部 2 2 0 1 との間の通信がインターネットや公衆網を用いる場合には、通信経路での配信データ内に含まれるコンテンツデータの盗聴を防止するための暗号化通信が望ましい。このような暗号化通信は、SSL（セキュア・ソケット・レイヤー）暗号化通信など、広く一般的に知られている技術で実現することが可能である。また、携帯情報端末 2 へ配信された配信データを悪意のユーザによる盗用から保護するためには、配信データメモリ 2 2 0 2 は本発明によるシステム以外からはアクセスできないこと、あるいは、暗号化により実質的にアクセスできないことが重要である。

#### バックアップ

図 7（A）は、安全化データ生成部 2 2 0 3 で生成され、送信時にコンテンツボディの暗号化を行わないと指定されたバックアップ用安全化データの構成例を示す模式図であり、（B）は、安全化データ生成部 2 2 0 3 で生成され、送信時にコンテンツボディの暗号化を行うと指定されたバックアップ用安全化データの構成例を示す模式図である。

図7 (A) に示す安全化データ701は、携帯情報端末2に格納されている端末識別情報 (IDt)、所有者識別情報 (IDu)、配信データに含まれる管理用ヘッダ (H)、コンテンツボディ (B) および流通制御情報

(P)、流通署名 (S1)、流通署名検証鍵 (vkt)、および端末証明書 (c\_vkt) を含んでいる。流通署名 (S1) は、端末識別情報 (IDt)、所有者識別情報 (IDu)、管理用ヘッダ (H)、コンテンツボディ (B)、および、流通制御情報 (P) を結合したデータに対して、携帯情報端末2に格納されている流通署名作成鍵 (skt) を用いて作成したデジタル署名である： $S1 = \text{Sig}[\text{skt}(\text{IDt} + \text{IDu} + \text{H} + \text{B} + \text{P})]$ 。

図7 (B) に示す安全化データ702は、送信時にコンテンツボディの暗号化を行うと指定された場合の安全化データであり、携帯情報端末2に格納されている端末識別情報 (IDt)、所有者識別情報 (IDu)、配信データに含まれる管理用ヘッダ (H)、コンテンツボディ (B) を暗号化した暗号化コンテンツボディ (E) および流通制御情報 (P)、流通署名 (S2)、流通署名検証鍵 (vkt)、および端末証明書 (c\_vkt) を含んでいる。ここで、暗号化コンテンツボディ (E) は、携帯情報端末2に格納されているコンテンツ暗号化鍵 (ek) を用いて作成する。また、流通署名 (S2) は、端末識別情報 (IDt)、所有者識別情報 (IDu)、管理用ヘッダ (H)、暗号化コンテンツボディ (E)、および、流通制御情報 (P) を結合したデータに対して、携帯情報端末2に格納されている流通署名作成鍵 (skt) を用いて作成したデジタル署名である： $S2 = \text{Sig}[\text{skt}(\text{IDt} + \text{IDu} + \text{H} + \text{E} + \text{P})]$ 。

このようにして生成されたバックアップ用安全化データ701または702は送受信部2207を通してユーザ情報端末3へ送信される。

ユーザ情報端末3において、送受信部2301は携帯情報端末2からバックアップ用安全化データを受信し、安全化データメモリ2302に記憶する。安全化データメモリ2302に記憶されるデータは、図7に示した安全化データを少なくとも含んでいればよく、それ以外の情報を併せて格納すること

も可能である。たとえば、保存日時情報を合わせて記憶しておけば、最後に転送した安全化データであることを識別することができる。

#### リストア

次に、ユーザ情報端末 3 に格納した安全化データを携帯情報端末 2 へ復元する動作について説明する。

##### 1) 安全化データリクエスト

図 8 は安全化データリクエスト生成部 2204 で生成する安全化データリクエストの構成例を示す模式図である。図 8 において安全化データリクエストは端末識別情報 (IDt')、所有者識別情報 (IDu')、コンテンツ暗号化鍵 (ek')、コンテンツ暗号化鍵証明書 (c\_\_ek') を含んで構成される。ここで記号「'」(ダッシュ) は、安全化データリクエストを生成する携帯情報端末の端末固有情報を、先に安全化データを作成した携帯情報端末の端末固有情報から区別するために付加したものである。すなわち、同一の携帯情報端末であれば端末固有情報は完全に一致するが、正当にあるいは不正に異なる携帯情報端末を用いて安全化データリクエストを生成した場合には、これら端末固有情報が一致しないことを考慮したものである。

安全化データリクエストには、図 8 に示した情報の他に、リクエストする安全化データを識別するための情報を含んでもよい。また、安全化データを識別する情報が含まれない場合には、ユーザ情報端末 3 で保存している安全化データを全てリクエストしたものと解釈する。あるいは、ユーザ情報端末 3 がユーザインタフェースを持つ場合には、それをユーザに操作させ、携帯情報端末 2 へ転送したい安全化データを選択してもよい。

安全化データリクエスト生成部 2204 で生成した安全化データリクエストは、送受信部 2207 を通して携帯情報端末 2 からユーザ情報端末 3 へ送信される。ユーザ情報端末 3 は、送受信部 2301 で安全化データリクエストを受信し、更新要否判定部 2303 へ転送する。

##### 2) 更新要否判定

更新要否判定部 2303 は、安全化データメモリ 2302 に記憶されてい

るバックアップ安全化データを読み出し、バックアップ安全化データに含まれる流通制御情報と、安全化データリクエストに含まれる端末識別情報および所有者識別情報とを比較する。この比較結果に応じて、バックアップ安全化データをそのまま携帯情報端末 2 へ転送するか、あるいは、サービス提供者サーバ 1 に転送判定および安全化データの更新要求を依頼するか否かを判定する。

図 9 は更新要否判定部 2303 の安全化データ更新判定動作の一例を示すフローチャートである。ここでは、ID 情報が端末識別情報 ID<sub>t</sub> および所有者識別情報 ID<sub>u</sub> からなり、さらに安全化データが図 6 (B) に示した流通制御情報を含んでいる場合を例示する。ID 情報がグループ ID あるいは家族 ID などからなる場合も同様である。

図 9 において、更新要否判定部 2303 は、まずバックアップ安全化データに含まれる端末識別情報 (ID<sub>t</sub>) と安全化データリクエストに含まれる端末識別情報 (ID<sub>t'</sub>) とを比較する (ステップ S1)。

15 ID<sub>t</sub> = ID<sub>t'</sub> であれば (ステップ S1 の YES)、続いてバックアップ安全化データに含まれる流通制御情報の同一端末間移動フラグ (F<sub>t</sub>) の値が「1: 許可」であるか否かを判定する (ステップ S2)。F<sub>t</sub> = 1 (同一端末間移動許可) であれば (ステップ S2 の YES)、バックアップ安全化データを送受信部 2301 を通してそのまま携帯情報端末 2 へ転送する (転送許可)。

20 F<sub>t</sub> ≠ 1 であれば (ステップ S2 の NO)、更新要否判定部 2303 は、さらに、バックアップ安全化データに含まれる流通制御情報の同一端末間移動フラグ (F<sub>t</sub>) の値が「2: サービス提供者サーバ問合せ」であるかを判定する (ステップ S3)。F<sub>t</sub> = 2 であれば (ステップ S3 の YES)、更新要否判定部 2303 は更新リクエスト生成部 2304 へバックアップ安全化データを転送し、後述するサーバ問合せ処理を開始する。F<sub>t</sub> ≠ 2 であれば (ステップ S3 の NO)、F<sub>t</sub> = 0 (転送禁止) と判断され、携帯情報端末 2 へのリストアは禁止される。

一方、 $IDt \neq IDt'$  であれば（ステップ S 1 の NO）、更新要否判定部 2303 は、バックアップ安全化データに含まれる所有者識別情報（ $IDu$ ）と安全化データリクエストに含まれる所有者識別情報（ $IDu'$ ）を比較する（ステップ S 4）。

- 5  $IDu = IDu'$  であれば（ステップ S 4 の YES）、続いてバックアップ安全化データに含まれる流通制御情報の同一所有者間移動フラグ（ $Fu1$ ）の値が「1：許可」であるか否かを判定する（ステップ S 5）。 $Fu1 = 1$ （同一所有者間移動許可）であれば（ステップ S 5 の YES）、バックアップ安全化データを送受信部 2301 を通してそのまま携帯情報端末 2 へ  
10 転送する（転送許可）。

- $Fu1 \neq 1$  であれば（ステップ S 5 の NO）、更新要否判定部 2303 は、さらに、バックアップ安全化データに含まれる流通制御情報の同一所有者間移動フラグ（ $Fu1$ ）の値が「2：サービス提供者サーバ問合せ」であるかを判定する（ステップ S 6）。 $Fu1 = 2$  であれば（ステップ S 6 の YES）、  
15  $S$ ）、更新要否判定部 2303 は更新リクエスト生成部 2304 へバックアップ安全化データを転送し、後述するサーバ問合せ処理を開始する。 $Fu1 \neq 2$  であれば（ステップ S 6 の NO）、 $Fu1 = 0$ （転送禁止）と判断され、携帯情報端末 2 へのリストアは禁止される。

- $IDu \neq IDu'$  であれば（ステップ S 4 の NO）、更新要否判定部 23  
20 03 は、バックアップ安全化データに含まれる流通制御情報の異ユーザー間移動フラグ（ $Fu2$ ）の値が「1：許可」であるか否かを判定する（ステップ S 7）。 $Fu2 = 1$ （異ユーザー間移動許可）であれば（ステップ S 7 の YES）、バックアップ安全化データを送受信部 2301 を通してそのまま携帯情報端末 2 へ転送する（転送許可）。

- 25  $Fu2 \neq 1$  であれば（ステップ S 7 の NO）、更新要否判定部 2303 は、さらに、異ユーザー間移動フラグ（ $Fu2$ ）の値が「2：サービス提供者サーバ問合せ」であるかを判定する（ステップ S 8）。 $Fu2 = 2$  であれば（ステップ S 8 の YES）、更新要否判定部 2303 は更新リクエスト生成

部 2 3 0 4 へバックアップ安全化データを転送し、後述するサーバ問合せ処理を開始する。Fu2≠2であれば（ステップS 8 のNO）、Fu2=0（転送禁止）と判断され、携帯情報端末 2 へのリストアは禁止される。

- 5       このように、バックアップ安全化データを携帯情報端末 2 へ転送するか（転送許可）、サービス提供者サーバに転送判定および安全化データの更新を依頼するか（サーバ問合せ）、あるいは、転送しないか（転送禁止）を判定することができる。ただし、判定方法はこれに限定されるものではない。流通制御情報に記録されている情報と安全化データリクエストに含まれる情報とを利用し、転送許可／サーバ問合せ／転送禁止が判定できれば他の判定
- 10     方法でもよい。なお、流通制御情報は、後述するように手続的に記述される場合もある。

### 3) サーバ問合せ

更新要否判定部 2 3 0 3 が「サーバ問合せ」と判定した場合、更新リクエスト生成部 2 3 0 4 は更新リクエストを生成する。

- 15     図 1 0 は更新リクエストの構成例を示す模式図である。更新リクエストは、少なくともバックアップ安全化データと安全化データリクエストとを含んでいる。なお、図 1 0 に示す更新リクエストでは、暗号化されていないコンテンツボディ（B）の場合と暗号化コンテンツボディ（E）の場合とが記載されている。送受信部 2 3 0 5 は生成された更新リクエストをサービス提供者
- 20     サーバ 1 へ送信する。

- サービス提供者サーバ 1 において、ユーザ情報端末 3 から更新リクエストを受信すると、流通署名検証鍵検証部 2 1 0 6 は更新リクエストに含まれる端末証明書（c\_v k t）を元に、流通署名検証鍵（v k t）がシステム管理者により割り当てられた正当な流通署名検証鍵であることを検証する。た
- 25     だし、流通署名検証鍵検証部 2 1 0 6 は端末証明書の正しさを検証するために必要な情報を保持しているものとする。

流通署名検証鍵（v k t）の正当性が否定された場合、サーバ問合せによる安全化データの更新は失敗し、携帯情報端末 2 への安全化データ転送の処



理（リストア）は中止する。

- 流通署名検証鍵（ $vkt$ ）の正当性が検証された場合、更新可否判定部 2107 は、更新リクエストに含まれる流通署名検証鍵（ $vkt$ ）によって、流通署名  $S1$  あるいは流通署名  $S2$  に基づいて端末識別情報（ $IDt$ ）、所有者識別情報（ $IDu$ ）、管理用ヘッダ（ $H$ ）、コンテンツボディ（ $B$ ）または暗号化コンテンツボディ（ $E$ ）、および、流通制御情報（ $P$ ）が改ざんされていない正しい情報であることを検証する。さらに、端末識別情報（ $IDt$ 、 $IDt'$ ）、所有者識別情報（ $IDu$ 、 $IDu'$ ）、管理用ヘッダ（ $H$ ）を元に、外部判定システム 2402 と連携して、バックアップ安全化データに含まれているコンテンツデータを端末識別情報  $IDt'$  の携帯情報端末へ転送して復元してよいか否かを判定する。バックアップ安全化データおよび転送先の携帯情報端末の正当性が確認されると、バックアップ安全化データの更新可能と判定される。

- バックアップ安全化データの更新が可能と決定された場合、コンテンツ暗号化鍵検証部 2108 は、更新リクエストに含まれるコンテンツ暗号化鍵証明書（ $c\_ek'$ ）を元に、コンテンツ暗号化鍵（ $ek'$ ）がシステム管理者により正しく割り当てられたコンテンツ暗号化鍵であることを検証する。なお、コンテンツ暗号化鍵検証部 2108 はコンテンツ暗号化鍵証明書の正しさを検証するために必要な情報を保持しているものとする。コンテンツ暗号化鍵（ $ek'$ ）の検証に失敗した場合は、サーバ問合せによる安全化データの更新は失敗し、携帯情報端末 2 への安全化データ転送の処理は中止する。

コンテンツ暗号化鍵（ $ek'$ ）の検証に成功した場合、安全化データ更改部 2109 は、配信データ生成部 2103 から配信データを取得して更新された安全化データを生成する。

- 図 11（A）は、安全化データ更改部 2109 で生成され、送信時にコンテンツボディの暗号化を行わないと指定された更新安全化データの構成例を示す模式図であり、（B）は、安全化データ更改部 2109 で生成され、送信時にコンテンツボディの暗号化を行うと指定された更新安全化データの構

成例を示す模式図である。

図11 (A) に示す安全化データ1101は、サービス提供者によって更新された安全化データであることを示すサービス提供者更新フラグ (F)、サービス提供者サーバに格納されているサービス提供者識別情報 (IDs)、  
5 配信データ生成部2103で改めて生成された配信データ (H"、B" およびP")、流通署名検証鍵 (vks)、サービス提供者証明書 (c\_vks)、および、流通署名 (S1") を含んでいる。

流通署名 (S1") は、サーバ固有情報格納部103に格納されている流通署名作成鍵 (sks) を用いて作成されるデジタル署名である。具体的には、配信データ生成部2103で改めて生成した配信データに含まれる管理  
10 用ヘッダ (H")、コンテンツボディ (B") および流通制御情報 (P") と、更新リクエストに含まれている端末識別情報 (IDt') と、サービス提供者更新フラグ (F) と、サービス提供者識別情報 (IDs) と、を結合したデータに対して、流通署名作成鍵 (sks) を用いて作成される：  
15  $S1" = \text{Sig}[sks(F + IDs + IDt' + H" + B" + P")]$ 。

図11 (B) に示す安全化データ1102は、サービス提供者によって更新された安全化データであることを示すサービス提供者更新フラグ (F)、サービス提供者サーバに格納されているサービス提供者識別情報 (IDs)、  
20 配信データ生成部2103で改めて生成された配信データ (H"、E" およびP")、流通署名検証鍵 (vks)、サービス提供者証明書 (c\_vks)、および、流通署名 (S2") を含んでいる。

流通署名 (S2") は、サーバ固有情報格納部103に格納されている流通署名作成鍵 (sks) を用いて作成されるデジタル署名である。具体的には、配信データ生成部2103で改めて生成した配信データに含まれる管理  
25 用ヘッダ (H")、コンテンツボディ (B") を暗号化した暗号化コンテンツボディ (E") および流通制御情報 (P") と、更新リクエストに含まれている端末識別情報 (IDt') と、サービス提供者更新フラグ (F) と、サービス提供者識別情報 (IDs) と、を結合したデータに対して、流通署

名作成鍵 ( $sks$ ) を用いて作成される:  $S2'' = \text{Sig}[sks(F + IDs + IDt' + H'' + E'' + P'')]$ 。なお、暗号化コンテンツボディは更新リクエストに含まれていて、検証されたコンテンツ暗号化鍵 ( $ek'$ ) を用いて作成する。

- 5      ここで、記号「"」（ツダッシュ）は、更新リクエストに含まれている配信データの管理用ヘッダ ( $H$ )、コンテンツボディ ( $B$ ) / 暗号化コンテンツボディ ( $E$ )、および、流通制御情報 ( $P$ ) と区別するためにつけたものである。上述したように、コンテンツメモリ 2101 に記憶されているコンテンツデータは外部コンテンツ処理システム 2401 によって更新される
- 10    場合があり、サービス提供者サーバ 1 から携帯情報端末 2 に配信した配信データとは異なる場合があることを意味している。もちろん外部コンテンツ処理システム 2401 による更新はなく、同一の配信データであってもよい。

このようにして更新された安全化データは送受信部 2105 を介してユーザ情報端末 3 へ送信される。更新された安全化データを受信すると、ユーザ

15    情報端末 3 は当該更新安全化データをリストア用安全化データとして携帯情報端末 2 へ送信する。

#### 4) 安全性確認およびリストア

携帯情報端末 2 において送受信部 2207 は、ユーザ情報端末 3 から更新安全化データを受信する。この受信した安全化データは、サービス提供者サーバ 1 による更新がない場合には図 7 に示すような安全化データ 701 また

20    は 702 であり、サービス提供者サーバ 1 による更新があった場合には図 11 に示すような安全化データ 1101 または 1102 である。

流通署名検証鍵検証部 2205 は、受信した安全化データに含まれる端末証明書 ( $c\_vkt$ ) を元に、流通署名検証鍵 ( $vkt$ ) がシステム管理者により正しく割り当てられた流通署名検証鍵であることを検証する。あるいは、受信した安全化データに含まれるサービス提供者証明書 ( $c\_vks$ ) を元に、流通署名検証鍵 ( $vks$ ) が、システム管理者により正しく割り当てられた流通署名検証鍵であることを検証する。なお、流通署名検証鍵検証

25

部 2 2 0 5 は端末証明書及びサービス提供者証明書の正しさを検証するために必要な情報を保持しているものとする。

データ安全性確認部 2 2 0 6 では、流通署名検証鍵検証部 2 2 0 5 で検証された流通署名検証鍵 (v k t または v k s) を用いて、安全化データに含まれる流通署名 (S 1 / S 2 または S 1' / S 2') を元に、受信した安全化データが改ざんされていないことを確認する。改ざんが検知されたら処理を中断する。改ざんされていない場合には、次に説明するデータ安全性確認が行われる。

図 1 2 はデータ安全性確認部 2 2 0 6 におけるデータ安全性確認動作の一例を示すフローチャートである。ここでは、ID 情報が端末識別情報 ID t および所有者識別情報 ID u からなり、さらに安全化データが図 6 (B) に示した流通制御情報を含んでいる場合を例示する。ID 情報がグループ ID あるいは家族 ID などからなる場合も同様である。

図 1 2 において、データ安全性確認部 2 2 0 6 は正当性が確認された安全化データにサービス提供者更新フラグ (F) が含まれるか否かを判定する (ステップ S 1 1)。サービス提供者更新フラグ (F) が含まれる場合は (ステップ S 1 1 の YES)、サービス提供者サーバ 1 による更新があると判断され、安全化データに含まれる端末識別情報 (ID t') と携帯情報端末 2 に記憶されている端末識別情報 (ID t'') とを比較する (ステップ S 1 2)。

ID t' = ID t'' であれば (ステップ S 1 2 の YES)、同一の携帯情報端末であるから、正当性が確認された安全化データに含まれる配信データ (H'', B'', P'') を復元し、配信データメモリ 2 2 0 2 に格納する (格納許可)。なお、正当性が確認された安全化データに暗号化コンテンツボディ (E'') が含まれている場合には、コンテンツ復号鍵 (d k'') を用いて復号し、管理用ヘッダ (H'')、コンテンツボディ (B'') および流通制御情報 (P'') からなる配信データを復元し、配信データメモリ 2 2 0 2 へ格納する。ここで、暗号化コンテンツボディを正しく復号するためには、コン

テンツ復号鍵 ( $d k'$ ) とコンテンツ復号鍵 ( $d k''$ ) が一致している必要がある。コンテンツ復号鍵の一致は、サービス利用者がコンテンツ暗号化鍵を管理し、システム管理者が生成して携帯情報端末へ格納するコンテンツ復号鍵を間接的に管理するか、サービス提供者が配信データに含まれる流通制御情報を工夫することで実現できる。

$I D t' \neq I D t''$  であれば (ステップ S 1 2 の NO)、配信データメモリ 2 2 0 2 への格納は禁止される (格納禁止)。

- また、サービス提供者更新フラグ (F) が含まれていない場合は (ステップ S 1 1 の NO)、サービス提供者サーバ 1 による更新がないと判断され、
- 10 安全化データに含まれる端末識別情報 ( $I D t$ ) と携帯情報端末に記憶されている端末識別情報 ( $I D t''$ ) とを比較する (ステップ S 1 3)。  $I D t = I D t''$  であれば (ステップ S 1 3 の YES)、さらに、安全化データに含まれる流通制御情報の同一端末間移動フラグ ( $F t$ ) の値が「1:許可」であるか否かを判定する (ステップ S 1 4)。
- 15  $F t = 1$  であれば (ステップ S 1 4 の YES)、上述したように配信データメモリ 2 2 0 2 への格納が許可される (格納許可)。なお、正当性が確認された安全化データに暗号化コンテンツボディ (E) が含まれている場合には、コンテンツ復号鍵 ( $d k$ ) を用いて復号し、管理用ヘッダ (H)、コンテンツボディ (B) および流通制御情報 (P) からなる配信データを復元し、配信データメモリ 2 2 0 2 へ
- 20 格納する。ここで、暗号化コンテンツボディを正しく復号するためには、コンテンツ復号鍵 ( $d k$ ) とコンテンツ復号鍵 ( $d k''$ ) が一致している必要がある。コンテンツ復号鍵の一致は、サービス利用者がコンテンツ暗号化鍵を管理し、システム管理者が生成して携帯情報端末へ格納するコンテンツ復号鍵を間接的に管理するか、サービス提供者が配信データに含まれる流通制
- 25 御情報を工夫することで実現できる。

$F t \neq 1$  であれば (ステップ S 1 4 の NO)、配信データメモリ 2 2 0 2 への格納は禁止される (格納禁止)。

$I D t \neq I D t''$  であれば (ステップ S 1 3 の NO)、さらに、安全化デ

ータに含まれる所有者識別情報（IDu）と携帯情報端末に記憶されている所有者識別情報（IDu'）とを比較する（ステップS15）。IDu=IDu'であれば（ステップS15のYES）、安全化データに含まれる流通制御情報の同一所有者間移動フラグ（Fu1）の値が「1：許可」であるか否かを判定する（ステップS16）。Fu1=1であれば（ステップS16のYES）、上述したように配信データメモリ2202への格納が許可される（格納許可）。Fu1≠1であれば（ステップS16のNO）、配信データメモリ2202への格納は禁止される（格納禁止）。

IDu≠IDu'であれば（ステップS15のNO）、さらに、安全化データに含まれる流通制御情報の異所有者間移動フラグ（Fu2）の値が「1：許可」であるか否かを判定する（ステップS17）。Fu2=1であれば（ステップS17のYES）、上述したように配信データメモリ2202への格納が許可される（格納許可）。Fu2≠1であれば（ステップS17のNO）、配信データメモリ2202への格納は禁止される（格納禁止）。

15 以上説明した例では、安全化データ生成部2203と安全化データ更改部2109におけるコンテンツボディの暗号化、および、データ安全性確認部2206におけるコンテンツボディの復号において、公開鍵暗号系のコンテンツ暗号化鍵とコンテンツ復号鍵とを直接用いている。公開鍵暗号系に特有の計算速度の問題を解決するため、例えば、暗号化時に対称鍵暗号系の対称鍵をランダムに生成し、コンテンツボディは対称鍵を用いて暗号化し、当該対称鍵をコンテンツ暗号化鍵で暗号化して暗号化コンテンツボディと共に安全化データに含めてもよい。この場合、復号時には、まず、コンテンツ復号鍵で対称鍵を復号し、ここで得た対称鍵でコンテンツボディを復号することができる。

## 25 システムの適用例

つぎに、本実施形態によるデジタル情報流通制御装置が想定する利用シーンの例を紹介する。

図13は本発明の第1実施形態によるデジタル情報流通制御システムの第

1の適用例を示す概略的システム機能図である。図13に示す利用シーンでは、システム管理者として携帯電話キャリア10、サービス提供者として携帯電話向けサービス事業者11、サービス利用者として携帯電話ユーザ12を想定している。

- 5 サービス提供者サーバ1は携帯電話2へ向けてコンテンツデータ（ここでは電子チケットを含むものとする。）を配信する。携帯電話ユーザ12は配信されたコンテンツを携帯電話2上で閲覧したり、電子チケットサービスターミナル13が設置されている場所へ赴き、携帯電話2内の電子チケットを利用することができる。また、上述したように、携帯電話ユーザ12は、赤
- 10 外線通信や近距離無線通信などを利用して、自分のパーソナルコンピュータ3（ユーザ情報端末）にデジタルコンテンツや電子チケットをバックアップし、必要に応じて携帯電話2へリストアする。このバックアップおよびリストアは、上述したように正当性および安全性が担保されているために、ユーザの利便性とサービス提供者の権利保護とを共に確保することができる。

15 システムの他の例

図1および図3に示す本発明の第1実施形態はハードウェアにより実現することもできるが、ソフトウェアによりコンピュータ上にインプリメントすることもできる。

- 図14は第1実施形態におけるサービス提供者サーバ1の他の例を示す概略的ブロック図であり、図15は第1実施形態における携帯情報端末2およびユーザ情報端末3の他の例を示す概略的ブロック図である。なお、図1および図3に示すブロックと同じ機能を有するものには同一の参照番号を付して説明は省略する。
- 20

- 図14に示すように、サービス提供者サーバ1には、コンテンツ・流通制御情報メモリ101、サーバ固有情報メモリ103、プログラムメモリ105、プログラム制御プロセッサ108、通信制御部109および送受信部110が設けられている。プログラムメモリ105には、配信データ管理部102と同じ機能を実現する配信データ管理プログラム106と、安全化デー
- 25

タ更新部 104 と同じ機能を実現する安全化データ更新プログラム 107 とが格納されている。

5 プログラム制御プロセッサ 108 は、プログラムメモリ 105 に格納されたプログラムを実行することで、図 2 に示すような携帯情報端末 2 へのデータ配信、外部コンテンツ処理システム 2401 によるコンテンツデータの更新、更新リクエストの受信、更新可否判定（ステップ S05）および安全化データの更新（ステップ S06）を実行する。特に、配信データ管理プログラム 106 を実行することによりデータ配信およびコンテンツデータの更新  
10 を実行する配信データ管理部 102 と、安全化データ更新プログラム 107 を実行することにより更新可否判定（ステップ S05）および安全化データの更新（ステップ S06）を実行する安全化データ更新部 104 と、をソフトウェア的に実現することができる。

また、上述した更新リクエストの受信、更新安全化データの送信、配信データの送信などの実際の通信は、プログラム制御プロセッサ 108 の制御の下で通信制御部 109 および送受信部 110 により実行される。  
15

図 15 に示すように、携帯情報端末 2 は、端末固有情報メモリ 202、配信データメモリ 2202、プログラムメモリ 205、プログラム制御プロセッサ 208、チャネル制御部 209、送受信器 210、通信制御部 211、および、ワイヤード／ワイヤレスインタフェース 212 を有する。

20 プログラムメモリ 205 には安全化データ検証プログラム 206 および安全化データ生成プログラム 207 が格納され、それぞれプログラム制御プロセッサ 208 により実行されることで、図 2 に示すような配信データの受信、配信データの保存／読み出し、安全化データ生成（ステップ S01）、安全化データリクエストの生成および送信、ユーザ情報端末 3 からの安全化データ  
25 の受信、受信した安全化データの安全性確認、および、安全性が確認された配信データのリストアを実行する。特に、安全化データ生成プログラム 207 を実行することで安全化データ生成（ステップ S01）を実行する安全化データ作成部 203 と、安全化データ検証プログラム 206 を実行するこ



とで安全性確認（ステップS 0 7）を実行する安全化データ検証部 2 0 4 とをソフトウェア的に実現することができる。サービス提供者サーバ 1 との通信はチャネル制御部 2 0 9 および送受信器 2 1 0 により実行し、ユーザ情報端末 3 との通信は通信制御部 2 1 1 およびインタフェース 2 1 2 により行う。

- 5      また、ユーザ情報端末 3 は、安全化データメモリ 3 0 1、ワイヤード／ワイヤレスインタフェース 3 0 3、通信制御部 3 0 4、プログラムメモリ 3 0 5、プログラム制御プロセッサ 3 0 7、通信制御部 3 0 8、および、送受信部 3 0 9 を有する。プログラムメモリ 3 0 5 には安全化データ更新判定プログラム 3 0 6 が格納され、プログラム制御プロセッサ 3 0 7 により実行されることで、図 1 に示すようなバックアップ安全化データの受信、バックアップ安全化データの格納（ステップS 0 2）、安全化データリクエストの受信、更新判定（ステップS 0 3）、更新リクエストの生成（ステップS 0 4）、および、更新安全化データの受信および転送を実行する。とくに、安全化データ更新判定プログラム 3 0 6 を実行することにより、更新判定（ステップ
- 10      S 0 3）を実行する安全化データ更新判定部 3 0 2 をソフトウェア的に実現することができる。サービス提供者サーバ 1 との通信は通信制御部 3 0 8 および送受信部 3 0 9 により実行し、携帯情報端末 2 との通信は通信制御部 3 0 4 およびインタフェース 3 0 3 により行う。
- 15

## 2. 第 2 実施形態

- 20      携帯情報端末 2 に格納された配信データを安全化データとしてバックアップし、必要に応じてリストアするシステムは、図 1 に示すような携帯情報端末 2 とユーザ情報端末 3 とを直接接続した構成に限定されるものではない。本発明によるバックアップおよびリストア動作は、携帯情報端末 2 とユーザ情報端末 3 とがネットワークを介して接続されたシステム構成においても可能である。
- 25

図 1 6 は本発明の第 2 実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。本実施形態によるシステムでは、図 1 におけるユーザ情報端末がネットワーク 5 に接続されたバックアップサー

バ 3 により実現されている。バックアップサーバ 3 の基本構成および動作は、第 1 実施形態のユーザ情報端末 3 と同じであるから説明は省略する。

図 1 7 は本発明の第 2 実施形態によるデジタル情報流通制御システムの適用例を示す概略的システム機能図である。図 1 7 に示す利用シーンでは、ユーザ情報端末が携帯電話ユーザ 1 2 のパーソナルコンピュータではなく、バックアップサービス事業者 1 4 が管理するバックアップサーバ 3 である。本発明によるバックアップやリストアは公衆網を介して行われる。

### 3. 第 3 実施形態

図 1 および図 3 に示す第 1 実施形態では、ユーザ情報端末 3 が、サービス提供者サーバ 1 へインターネットなどのネットワーク 5 で接続され、安全化データの更新ができる場合を説明した。しかしながら、本発明はこのような構成に限定されるものではない。たとえば、安全化データ更新判定部 3 0 2 に含まれる更新要否判定機能、更新リクエスト生成機能、更新リクエスト送信機能などを携帯情報端末 2 に持たせることもできる。この場合には、ユーザ情報端末 3 はサービス提供者サーバ 1 へ接続する通信機能が不要となる。

図 1 8 は本発明の第 3 実施形態によるデジタル情報流通制御システムを示す概略的システム機能図である。なお、図 1 および図 3 に示すブロックと同じ機能を有するものには同一の参照番号を付して説明は省略する。図 1 9 は、図 1 8 のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。なお図 2 に示す流れ図と同じ動作ステップには同じ参照番号を付している。

図 1 8 および図 1 9 に示すように、本実施形態における携帯情報端末 2 には、安全化データ更新判定部 2 2 0 が設けられ、ユーザ情報端末 3 には安全化データ格納部 3 0 1 の一般的なデータ入出力制御を行う制御部 3 1 0 が設けられている。配信データが携帯情報端末 2 の配信データ格納部 2 0 1 に格納され、バックアップ時には配信データと端末固有情報とを利用してバックアップ用の安全化データが作成され（ステップ S 0 1）、ユーザ情報端末 3 の安全化データ格納部 3 0 1 に格納される（ステップ S 0 2）。

リストア時に携帯情報端末 2 から安全化データリクエストがユーザ情報端末 3 へ出力され、それにより制御部 3 1 0 は安全化データ格納部 3 0 1 から対応するバックアップ安全化データを読み出し、携帯情報端末 2 の安全化データ更新判定部 2 2 0 へ送信する。安全化データ更新判定部 2 2 0 は、安全化データリクエストの識別情報とバックアップ安全化データの識別情報および流通制御情報とを用いて、バックアップ安全化データをそのまま使用できるか否か、それともサービス提供者サーバ 1 への問い合わせが必要か否かを判断する（ステップ S 0 0 1）。すなわち、ステップ S 0 0 1 は図 2 のステップ S 0 3 と同様の動作を行う。バックアップ安全化データをそのまま使用できる場合は、上述した検証（ステップ S 0 7）を経て配信データ格納部 2 0 1 にリストアされる。

問い合わせが必要であれば、バックアップ安全化データおよび安全化データリクエストから更新リクエストを生成し（ステップ S 0 0 2）、送受信部 2 2 1 を通してサービス提供者サーバ 1 へ送信する。サービス提供者サーバ 1 から更新安全化データが帰ってくると、それを安全化データ検証部 2 0 4 へ出力し、上述した検証（ステップ S 0 7）を経て配信データ格納部 2 0 1 にリストアされる。

4. 第 4 実施形態 図 1 1 (A) および (B) において説明したように、サービス提供者によって更新された安全化データにはサービス提供者更新フラグ (F) が設定されている。第 1 実施形態ではこの更新フラグ F によって更新の有無を判定したが、単に更新の有無を示すフラグとしてだけでなく、安全化データのリストア可能な有効期限を示す情報としても利用することができる。

本発明の第 4 実施形態では、サービス提供者サーバ 1 において更新安全化データに有効期限情報が付加される。この場合のデータ安全性確認部 2 2 0 6 の動作は次のようになる。

図 2 0 は、有効期限情報を含む更新安全化データを受信したときのデータ安全性確認部 2 2 0 6 のデータ安全性確認動作の一例を示すフローチャート

である。なお、図 1 2 のフローチャートと同じステップは同じ参照番号を付して説明は省略する。

ユーザ情報端末 3 から受信した安全化データに更新フラグ F が含まれている場合には（ステップ S 1 1 の Y E S）、データ安全性確認部 2 2 0 6 はその更新フラグ F に付加された有効期限情報を読み取り、携帯情報端末 2 内の時計から読み出した現時刻情報と比較する（ステップ S 2 0）。現時刻が更新安全化データの有効期限内であれば（ステップ S 2 0 の Y E S）、ステップ S 1 2 が実行され、上述したように更新安全化データの格納が禁止あるいは許可される。現時刻が更新安全化データの有効期限を超えていれば（ステップ S 2 0 の N O）、更新安全化データの格納は禁止される。

このように、サービス提供者更新フラグ F の有効期限情報を参照してリストアの可否を判定することにより、安全化データ更改部 2 1 0 9 で生成した安全化データを悪意ある利用者がユーザ情報端末 3 に蓄積し、有効期限を超えて携帯情報端末 2 へ繰り返しリストアすることを防止できる。上述したように、サービス提供者サーバ 1 で更新された安全化データを悪意のプログラムが盗み、それを同一の携帯情報端末にリストアすることは可能である。このような不正なリストアを防止するために、サービス提供者更新フラグ F に設定される有効期限をたとえば安全化データの更新から 1 0 秒後などの非常に短時間に設定することは有効である。

## 20 5. 第 5 実施形態

第 1 実施形態で説明したように、ユーザ情報端末 3 に保存されているバックアップ安全化データをリストアしようとする際、携帯情報端末 2 の安全化データリクエスト生成部 2 2 0 4 は、端末識別情報（I D t'）、所有者識別情報（I D u'）、および、必要に応じてコンテンツ暗号化鍵（e k'）およびコンテンツ暗号化鍵証明書（c \_ e k'）を含む安全化データリクエストを生成する（図 8 参照）。さらに、この安全化データリクエスト自体に固有情報を付加することで、不正なリストアを有効に防止することが可能である。

図 2 1 は本発明の第 5 実施形態における安全化データリクエストの構成例を示す模式図である。本実施形態における安全化データリクエストは、端末識別情報 (ID t')、所有者識別情報 (ID u')、コンテンツ暗号化鍵 (ek')、コンテンツ暗号化鍵証明書 (c\_ek')、および、乱数 r を含んで構成される。

本実施形態における安全化データリクエスト生成部 2 2 0 4 は、乱数発生器から発生した乱数 r を入力して安全化データリクエストに付加すると共に、この乱数 r を保持しておく。乱数 r を含む安全化データリクエストがユーザ情報端末 3 へ送信され、サーバ問合せが必要であれば、更新リクエスト生成部 2 3 0 4 はバックアップ安全化データと安全化データリクエストとを組み合わせた更新リクエストを生成する (図 1 0 参照)。したがって、本実施形態では、更新リクエストの安全化データリクエストの部分には乱数 r が含まれている。この更新リクエストがサービス提供者サーバ 1 へ送信される。

図 1 1 (A) および (B) において説明したように、サービス提供者によって更新された安全化データにはサービス提供者更新フラグ (F) が設定されている。第 1 実施形態ではこの更新フラグ F によって更新の有無を判定したが、単に更新の有無を示すフラグとしてだけでなく、乱数 r を示す情報としても利用することができる。本実施形態では、サービス提供者サーバ 1 において更新安全化データの更新フラグ F に乱数 r の情報が付加される。この場合のデータ安全性確認部 2 2 0 6 の動作は次のようになる。

図 2 2 は、乱数 r を含む更新安全化データを受信したときのデータ安全性確認部 2 2 0 6 のデータ安全性確認動作の一例を示すフローチャートである。なお、図 1 2 のフローチャートと同じステップは同じ参照番号を付して説明は省略する。

ユーザ情報端末 3 から受信した安全化データに更新フラグ F が含まれている場合には (ステップ S 1 1 の YES)、データ安全性確認部 2 2 0 6 はその更新フラグ F に付加された乱数 r' を読み取り、安全化データリクエスト生成時に保持された乱数 r'' と比較する (ステップ S 2 1)。r' = r'' で

あれば（ステップS 2 1のYES）、ステップS 1 2が実行され、上述したように更新安全化データの格納が禁止あるいは許可される。 $r' \neq r''$ であれば（ステップS 2 1のNO）、更新安全化データの格納は禁止される。

- 5      このように、サービス提供者更新フラグFの乱数情報を参照してリストアの可否を判定することにより、安全化データ更改部2 1 0 9で生成した安全化データを悪意ある利用者がユーザ情報端末3に蓄積し、携帯情報端末2へ繰り返しリストアすることを防止できる。本実施形態では、携帯情報端末2に信頼できる時計がない場合でも不正なリストアを有効に防止できる。

#### 6. 第6実施形態

##### 10      流通制御情報の他の例

図6（A）に示す流通制御情報（P）は、図6（B）に示すようなフラグ構成だけではない。流通制御情報（P）をプログラムの関数として手続き的に記述することも可能である。

- 15      図2 3は、プログラムの関数として記述した流通制御情報の一例を示す模式図である。ここでは、流通制御情報がC++プログラミング言語で記述されており、「端末識別情報が一致した場合にはリストア許可、サービス提供者が指定する特別な日（ここでは2 0 0 4年2月1 4日）に所有者識別情報が一致した場合にはサーバ問い合わせ後リストア許可、それ以外はリストア不許可」という内容の流通制御を行うことができる。

- 20      このようにプログラムで流通制御情報を記述した場合には、更新要否判定部2 3 0 3およびデータ安全性確認部2 2 0 6は、この流通制御プログラムを読み込んで実行することとなり、図9および図1 2に示すフラグベースの更新要否判定およびデータ安全性確認に比べて柔軟な流通制御が可能となる。

## 請 求 の 範 囲

1. デジタル情報の配信サービスを行うサーバと、前記デジタル情報の  
配信サービスを受ける情報処理端末と、を有するシステムにおけるデジタル  
5 情報の流通制御方法において、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信  
データを前記サーバから前記情報処理端末へ配信し、

前記情報処理端末に前記配信データを格納し、

前記流通制御情報に従って前記情報処理端末と他の情報処理端末との間で  
10 の前記配信データを含む情報の転送を制御する、  
ことを特徴とするデジタル情報の流通制御方法。

2. 前記転送制御では、

前記情報処理端末の固有情報を用いて生成された前記配信データを含む情  
報を前記他の情報処理端末へ転送して格納し、

15 前記他の情報処理端末に格納された配信データを含む情報を前記情報処理  
端末へ再格納する前に、前記流通制御情報に従って前記情報処理端末への再  
格納の可否を判定する、

ことを特徴とする請求の範囲第1項記載の流通制御方法。

3. 前記転送制御では、

20 前記情報処理端末の固有情報を用いて生成された前記配信データを含む情  
報を前記他の情報処理端末へ転送して格納し、

前記他の情報処理端末に格納された配信データを含む情報を前記情報処理  
端末へ再格納する前に、前記流通制御情報に従って前記サーバへの問合せの  
可否を判定する、

25 ことを特徴とする請求の範囲第1項記載の流通制御方法。

4. 前記流通制御情報は、前記配信データを含む情報の転送可否決定条  
件および前記サーバへの問合せの可否決定条件のうち少なくとも1つを含む  
ことを特徴とする請求の範囲第1項記載の流通制御方法。

5. デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末とを有するシステムにおけるデジタル情報の流通制御方法において、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信  
5 データを前記サーバから前記情報処理端末へ配信し、

前記情報処理端末に前記配信データを格納し、

前記情報処理端末に割り当てられた端末固有情報を用いて前記配信データを含む第1安全化データを生成して他の情報処理端末へ転送し、

前記他の情報処理端末に格納された安全化データに含まれる配信データを  
10 前記情報処理端末へ再格納する前に、安全化データ送信要求を前記他の情報処理端末へ送信し、

前記情報処理端末の端末固有情報と、前記安全化データ送信要求に対応する第2安全化データに含まれる端末固有情報および流通制御情報とに基づいて、当該第2安全化データに含まれる配信データを前記情報処理端末へ再格  
15 納可能か否かを判定し、

再格納可能であるときに前記第2安全化データに含まれる前記配信データを前記情報処理端末に格納する、

ことを特徴とするデジタル情報の流通制御方法。

6. 前記流通制御情報は、安全化データの転送可否決定条件および前記  
20 サーバへの問合せの可否決定条件のうち少なくとも1つを指示することを特徴とする請求の範囲第5項記載の流通制御方法。

7. 前記第2安全化データの流通制御情報によりサーバ問合せが指定されている場合には、当該第2安全化データおよび前記安全化データ送信要求を含む安全化データ問合せを前記サーバに対して送信することを特徴とする  
25 請求の範囲第6項記載の流通制御方法。

8. 前記サーバは、

前記安全化データ問合せを受信すると、前記安全化データ問合せに含まれる第2安全化データの更新可否を判定し、



更新可能な場合には、当該サーバに割り当てられたサーバ固有情報を用いて当該第2安全化データを更新した更新安全化データを生成し、当該更新安全化データを前記安全化データ問合せに対する応答として返送し、

5 前記情報端末は、前記更新安全化データを前記安全化データ送信要求に対応する第2安全化データとして受信することを特徴とする請求の範囲第7項記載の流通制御方法。

9. 前記更新安全化データは有効期限情報を含み、

10 前記情報処理端末は、前記情報処理端末の端末固有情報と前記第2安全化データに含まれる端末固有情報、有効期限情報および流通制御情報とに基づいて、当該配信データを前記情報処理端末へ再格納可能か否かを判定する、ことを特徴とする請求の範囲第8項記載の流通制御方法。

10. 前記情報処理端末は、さらに、前記安全化データ送信要求に当該要求特定情報を付加して前記他の情報処理端末へ送信し、

15 前記サーバは前記更新安全化データに前記要求特定情報を含めて返送し、前記情報処理端末は、前記情報処理端末の端末固有情報と前記第2安全化データに含まれる端末固有情報、要求特定情報および流通制御情報とに基づいて、当該配信データを前記情報処理端末へ再格納可能か否かを判定する、ことを特徴とする請求の範囲第8項記載の流通制御方法。

20 11. 前記要求特定情報は、前記データ送信要求時に発生した乱数であることを特徴とする請求の範囲第10項記載の流通制御方法。

12. 前記流通制御情報は、データ転送の可否決定条件、情報転送時の暗号化の可否決定条件、および、前記サーバへの問合せの可否決定条件のうち少なくとも1つを指示することを特徴とする請求の範囲第5項記載の流通制御方法。

25 13. 前記端末固有情報は、流通署名作成鍵、流通署名検証鍵、端末証明書、暗号化鍵、暗号化鍵証明書、復号鍵、および、識別情報のうち少なくとも前記識別情報を含むことを特徴とする請求の範囲第12項記載の流通制御方法。

1 4. 前記情報処理端末は、

前記流通制御情報がデータ転送時の暗号化を指示している場合は、前記端末固有情報に含まれる前記暗号化鍵を用いて前記配信データに含まれるデジタル情報を暗号化し、

- 5 暗号化されたデジタル情報を含む配信データを用いて前記第1安全化データを生成して前記他の情報処理端末へ転送し、

前記第2安全化データに含まれる前記配信データの暗号化されたデジタル情報を前記端末固有情報に含まれる前記復号鍵を用いて復号する、

ことを特徴とする請求の範囲第13項記載の流通制御方法。

- 10 1 5. デジタル情報の配信サービスを行うサーバから前記デジタル情報の配信を受け、バックアップ用の他の情報処理端末との間でデータ転送可能な携帯情報端末において、

データ転送を制限する条件を示す流通制御情報と前記デジタル情報とを含む配信データを前記サーバから受信し格納する配信データ格納手段と、

- 15 当該携帯情報端末に割り当てられた端末固有情報を格納する端末固有情報格納手段と、

前記配信データ格納手段から前記他の情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第1安全化データを生成し、前記他の情報処理端末へ送信する安全化データ生成手段と、

- 20 前記他の情報処理端末から第2安全化データを受信して当該第2安全化データに含まれる配信データを前記配信データ格納手段へ再格納する前に、前記他の情報処理端末へデータ送信要求を行うデータ送信要求生成手段と、

- 前記データ送信要求の応答として前記他の情報処理端末から前記第2安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第2安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第2安全化データが再格納可能か否かを検証し、再格納可能であるときに前記第2安全化データに含まれる配信データを前記配信データ格納手段に格納する安全化データ検証手段と、
- 25

を有することを特徴とする携帯情報端末。

16. さらに、

前記データ送信要求の応答として前記他の情報処理端末から前記第2安全  
化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第2安  
5 全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第  
2安全化データの前記配信データ格納手段への転送可否を判定する判定手段  
を有し、

前記第2安全化データを前記配信データ格納手段への転送可能であれば、  
前記安全化データ検証手段により当該第2安全化データが再格納可能か否か  
10 を検証することを特徴とする請求の範囲第15項記載の携帯情報端末。

17. 前記流通制御情報は、データ転送の可否決定条件および前記サー  
バへの問合せの可否決定条件のうち少なくとも1つを指示することを特徴と  
する請求の範囲第16項記載の携帯情報端末。

18. 前記判定手段は、前記第2安全化データの流通制御情報によりサ  
ーバ問合せが指定されている場合には、前記データ送信要求および前記第2  
15 安全化データを含む安全化データ問合せを前記サーバに対して送信すること  
を特徴とする請求の範囲第17項記載の携帯情報端末。

19. 情報処理端末に対してデジタル情報の配信サービスを行うサーバ  
において、

20 当該サーバに割り当てられたサーバ固有情報を格納するサーバ固有情報格  
納手段と、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信  
データを生成して前記情報処理端末へ配信する配信データ管理手段と、

前記情報処理端末の端末固有情報および要求された安全化データを含む安  
25 全化データ問合せを受信すると、当該安全化データ問合せに含まれる前記安  
全化データの更新可否を判定し、更新可能な場合に当該安全化データを更新  
して前記安全化データ問合せの応答として返送する安全化データ更新手段と、  
を有することを特徴とするサーバ。

20. データ転送を制限する条件を示す流通制御情報とデジタル情報とを含む配信データをサーバから受信する携帯情報端末と接続可能であり、前記携帯情報端末が受信した前記配信データをバックアップする情報処理装置であって、

- 5 前記携帯情報端末に割り当てられた端末固有情報を用いて生成された前記配信データを含む第1安全化データを格納する安全化データ格納手段と、

前記安全化データ格納手段に格納された第1安全化データに含まれる配信データを前記携帯情報端末へ再格納するための安全化データ送信要求を前記携帯情報端末から受信し、当該受信したデータ送信要求と前記安全化データ格納手段に格納された第1安全化データの端末固有情報および流通制御情報  
10 とに基づいて、当該格納された第1安全化データを第2安全化データとして前記携帯情報端末へ返送するか否かを判定する判定手段と、

を有することを特徴とする情報処理装置。

21. デジタル情報の配信サービスを行うサーバと、前記デジタル情報の  
15 の配信を受ける第1情報処理端末と、前記第1情報処理端末との間でデータ転送可能な第2情報処理端末と、を少なくとも有する流通制御システムにおいて、

- 前記サーバは、データ転送を制限する条件を示す流通制御情報を前記デジタル情報に付加した配信データを生成して前記第1情報処理端末へ送信する  
20 配信データ管理手段を少なくとも有し、

前記第1情報処理端末は、

前記配信データを格納する配信データ格納手段と、

前記第1情報処理端末に割り当てられた端末固有情報を格納する端末固有情報格納手段と、

- 25 前記配信データ格納手段から前記第2情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第1安全化データを生成し、前記第2情報処理端末へ送信する安全化データ生成手段と、  
前記第2情報処理端末から第2安全化データを受信して当該第2安全化デ

ータに含まれる配信データを前記配信データ格納手段へ再格納するために、  
前記第 2 情報処理端末へデータ送信要求を行うデータ送信要求生成手段と、

- 前記データ送信要求の応答として前記第 2 情報処理端末から前記第 2 安全  
化データを受信すると、前記端末固有情報を用いて当該第 2 安全化データが  
5 再格納可能か否かを検証し、再格納可能であるときに前記第 2 安全化データ  
に含まれる配信データを前記配信データ格納手段に格納する安全化データ検  
証手段と、を少なくとも有し、

前記第 2 情報処理端末は、

- 前記第 1 情報処理端末から転送された前記第 1 安全化データを格納する安  
10 全化データ格納手段と、

前記データ送信要求と前記安全化データ格納手段に格納された安全化デー  
タの端末固有情報および流通制御情報とに基づいて、当該格納された安全化  
データを第 2 安全化データとして前記第 1 情報処理端末へ返送するか否かを  
判定する判定手段と、を少なくとも有する、

- 15 ことを特徴とする流通制御システム。

2 2. コンピュータに、情報処理端末に対してデジタル情報の配信サー  
ビスを行うサーバ機能を実現するためのサーバプログラムにおいて、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信  
データを生成して前記情報処理端末へ配信するステップと、

- 20 前記情報処理端末の端末固有情報および要求された安全化データを含む安  
全化データ問合せを受信すると、当該安全化データ問合せに含まれる前記安  
全化データの更新可否を判定するステップと、

更新可能な場合に当該安全化データを更新して前記安全化データ問合せの  
応答として返送するステップと、

- 25 を有することを特徴とするサーバプログラム。

2 3. コンピュータに、デジタル情報の配信サービスを行うサーバから  
前記デジタル情報の配信を受けると共にバックアップ用の他の情報処理端末  
との間でデータ転送を実行させる携帯情報端末用のプログラムにおいて、

データ転送を制限する条件を示す流通制御情報と前記デジタル情報とを含む配信データを前記サーバから受信し格納するステップと、

前記他の情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第 1 安全化データを生成し、前記他の情報処理端末へ送信するステップと、

前記他の情報処理端末から第 2 安全化データを受信して当該第 2 安全化データに含まれる配信データを前記配信データ格納手段へ再格納する前に、前記他の情報処理端末へデータ送信要求を行うステップと、

前記データ送信要求の応答として前記他の情報処理端末から前記第 2 安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第 2 安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第 2 安全化データが再格納可能か否かを検証するステップと、

再格納可能であるときに前記第 2 安全化データに含まれる配信データを格納するステップと、

を有することを特徴とする携帯情報端末用のプログラム。

24. 前記データ送信要求の応答として前記他の情報処理端末から前記第 2 安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第 2 安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第 2 安全化データの配信データ格納手段への転送可否を判定するステップと、

前記第 2 安全化データを前記配信データ格納手段への転送可能であれば、前記安全化データ検証手段により当該第 2 安全化データが再格納可能か否かを検証するステップと、

を更に有することを特徴とする請求の範囲第 23 項記載の携帯情報端末用のプログラム。

Fig.1

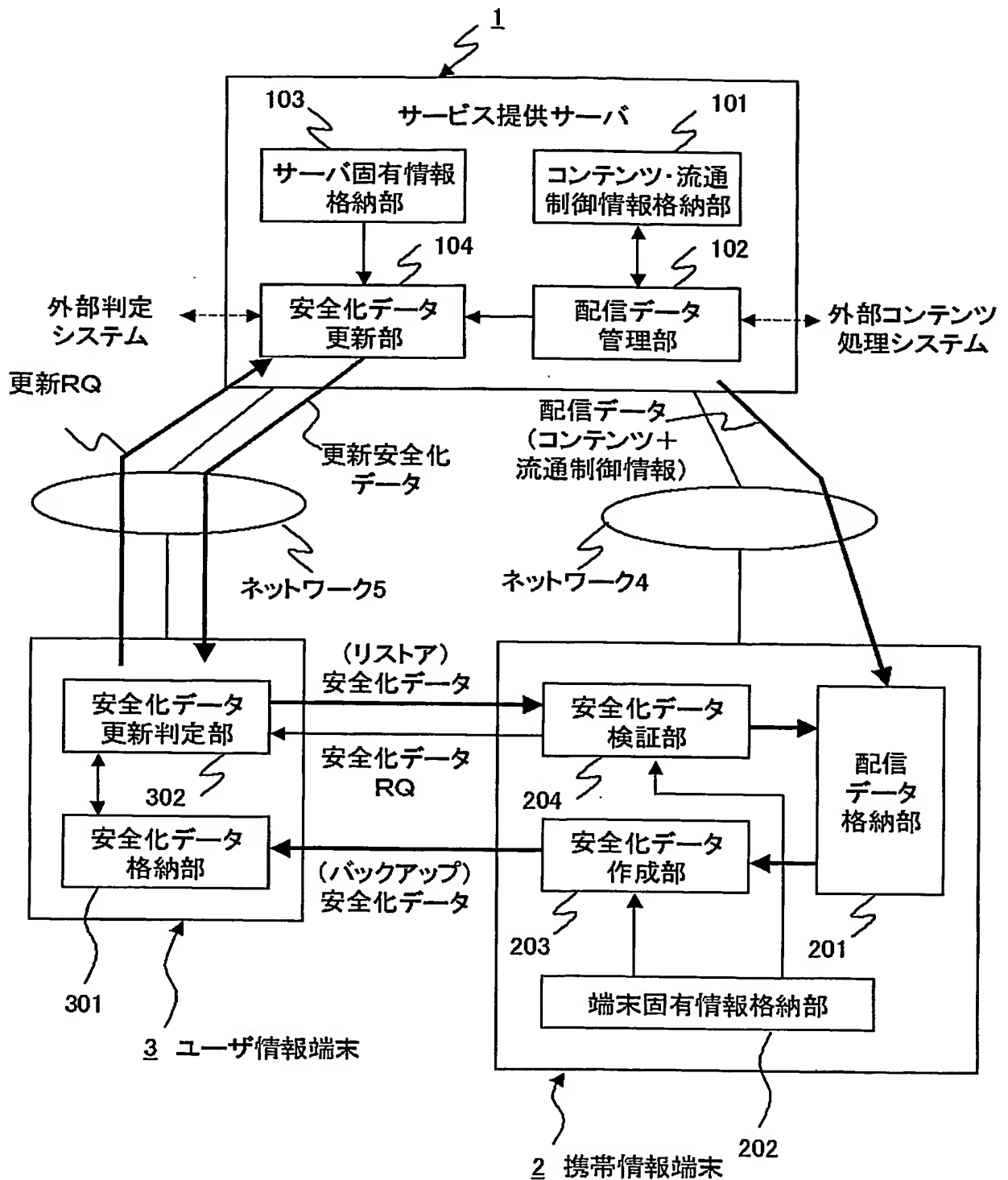
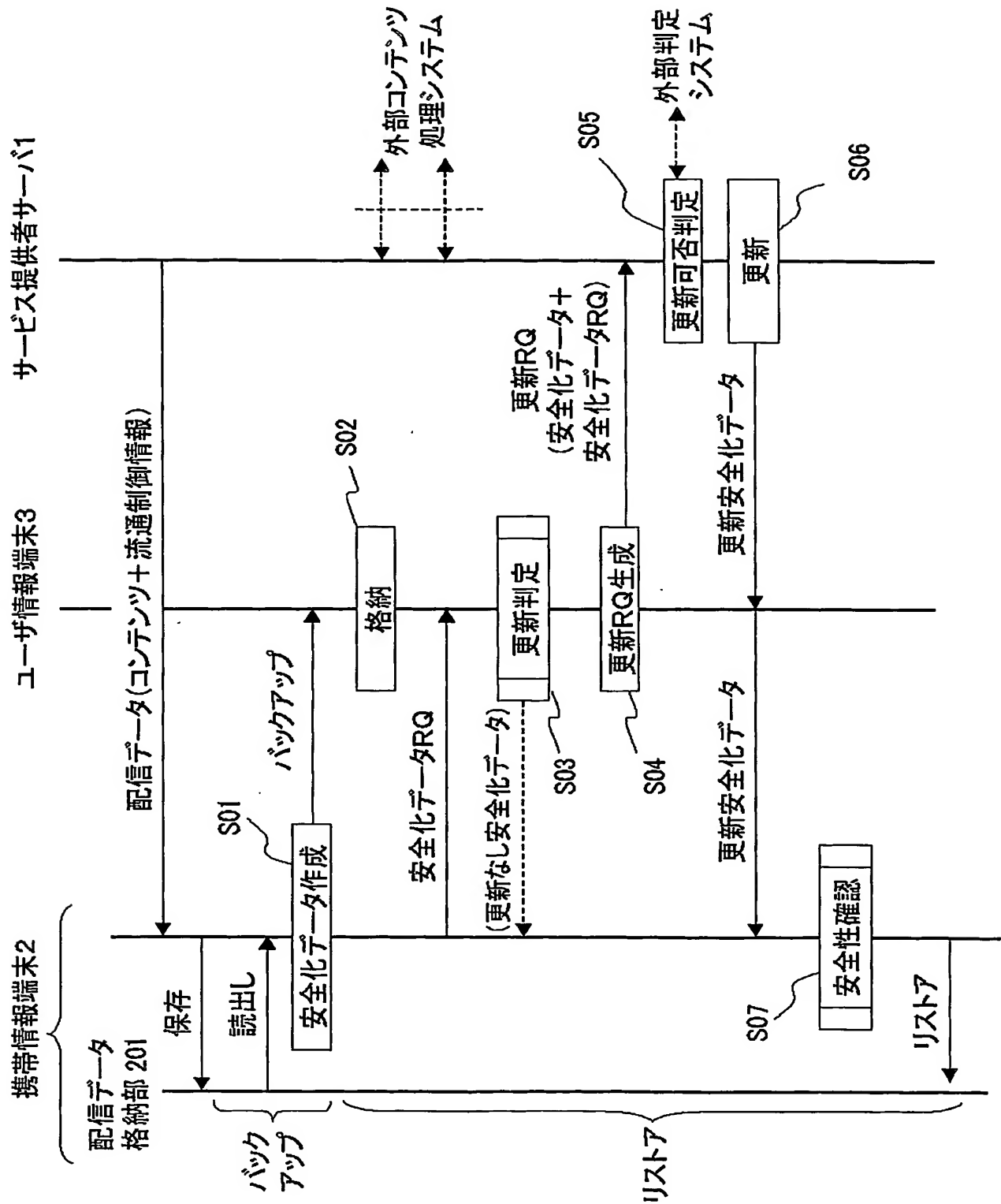


Fig.2





**Fig.3**

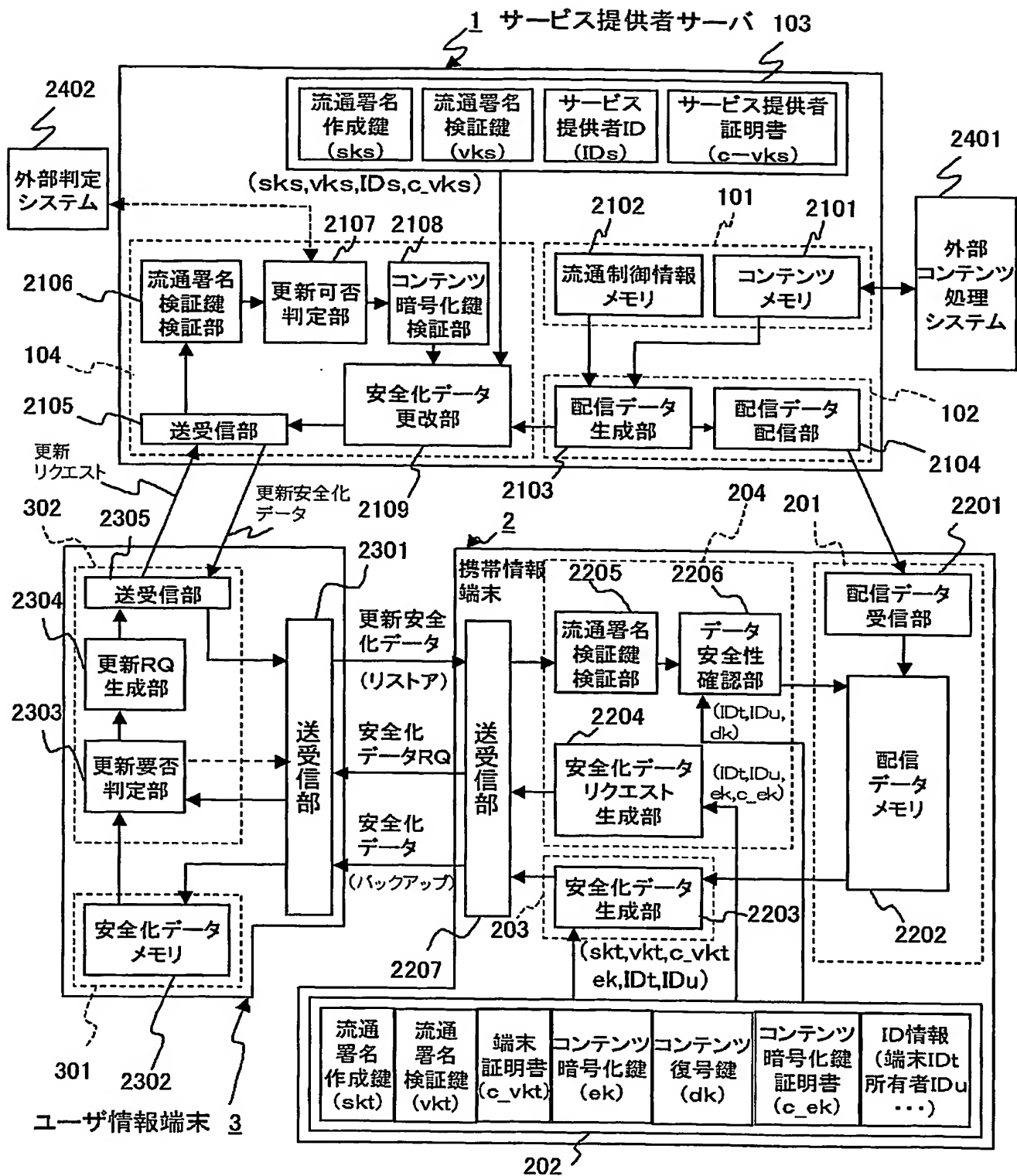


Fig.4

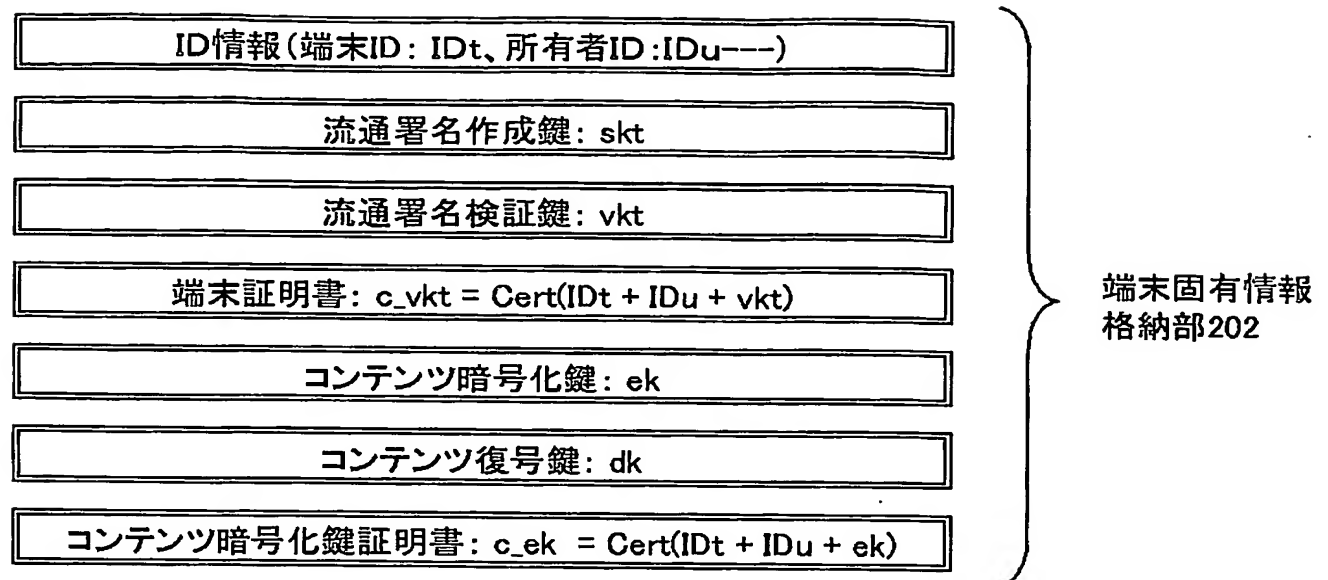
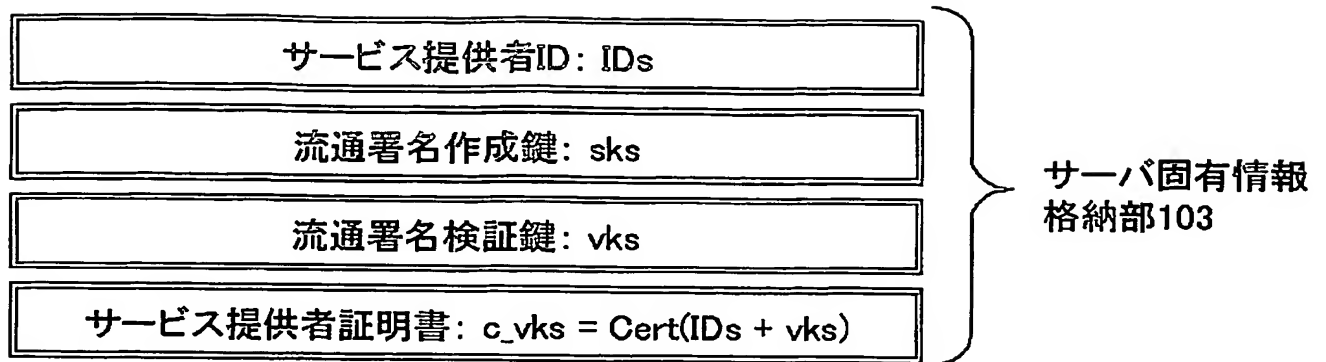


Fig.5



6 / 23

Fig.6

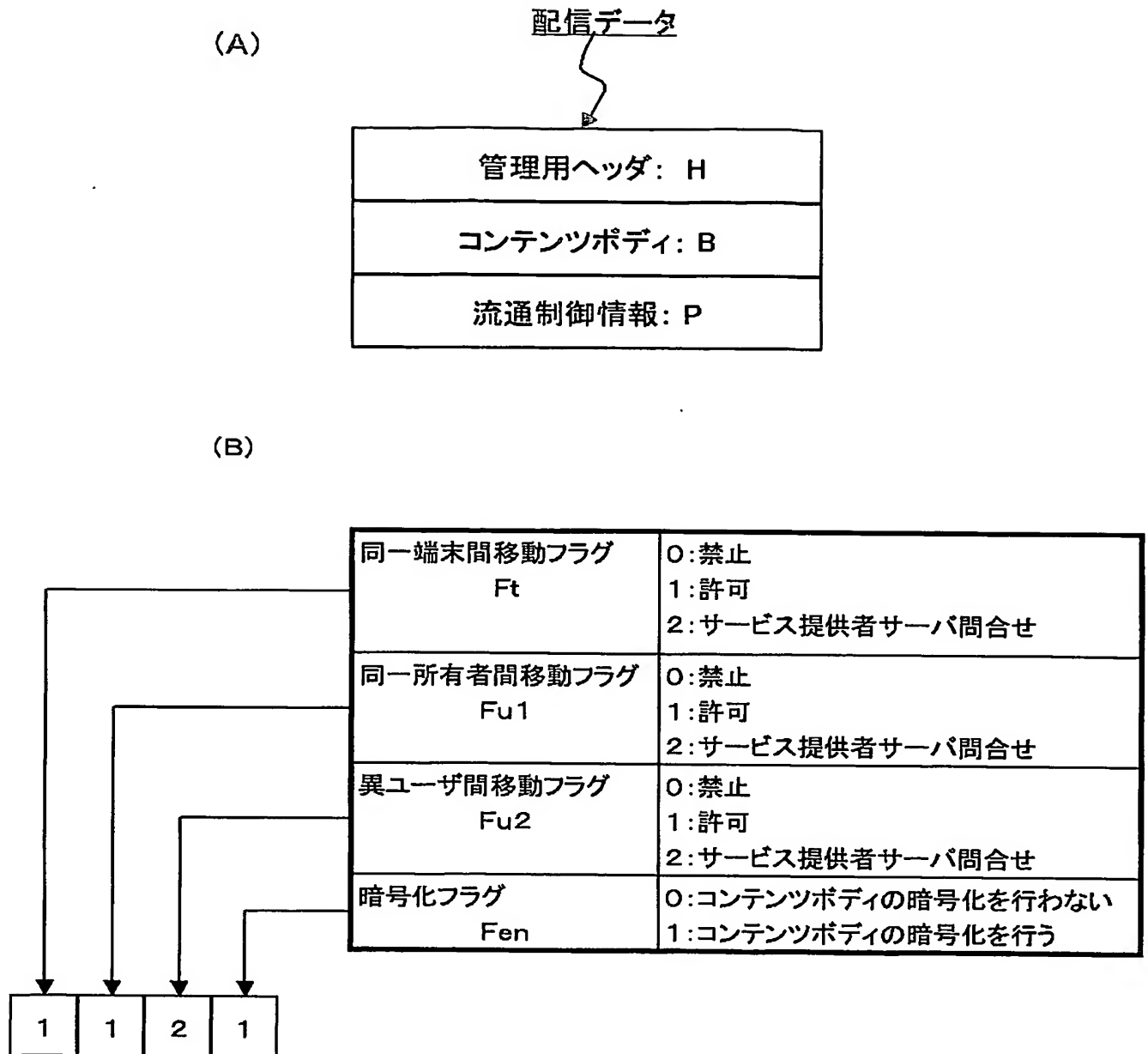


Fig.7

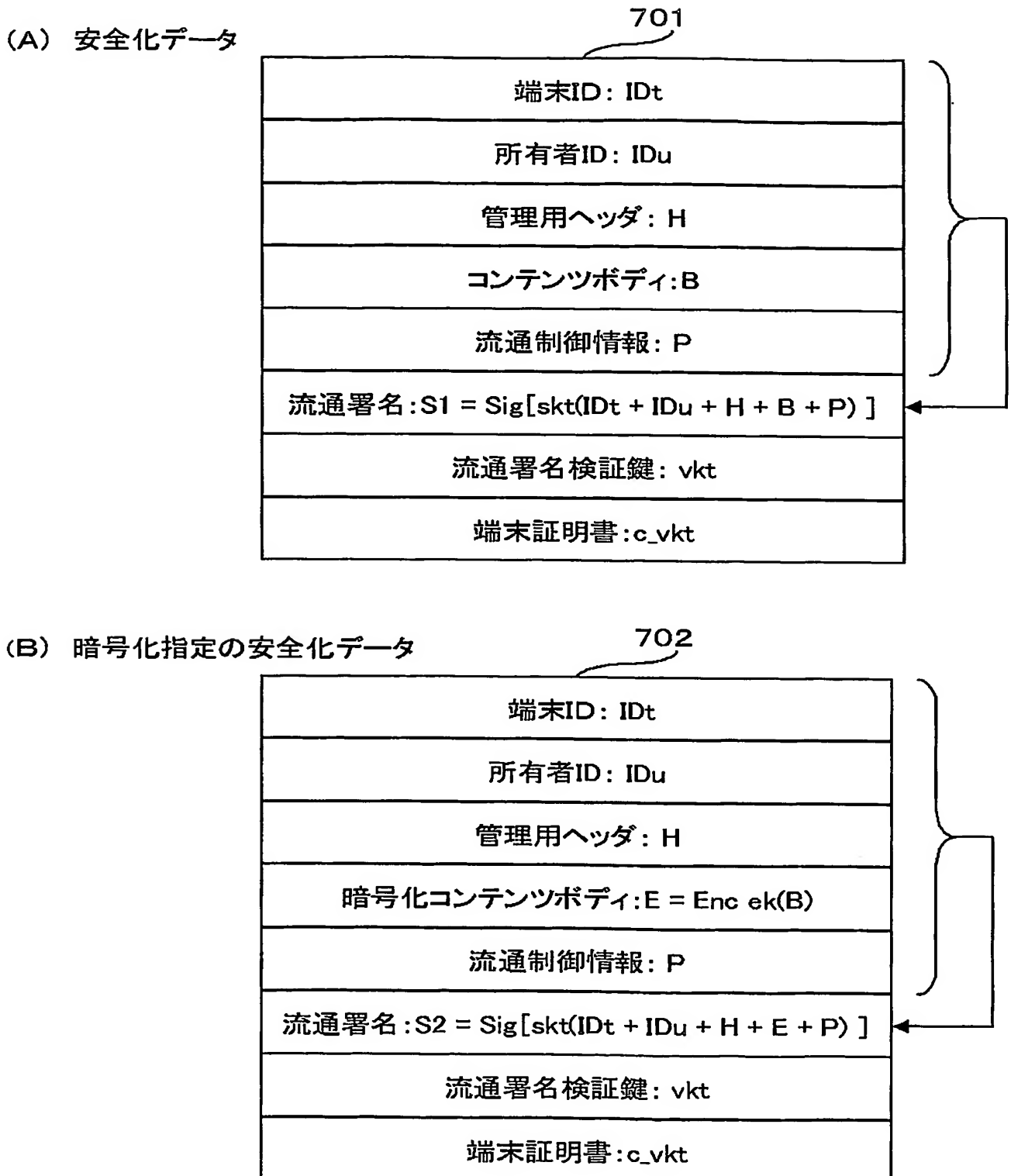


Fig.8

安全化データリクエスト



端末ID: IDt'
所有者ID: IDu'
コンテンツ暗号化鍵: ek'
コンテンツ暗号化鍵証明書: c_ek'

Fig.9

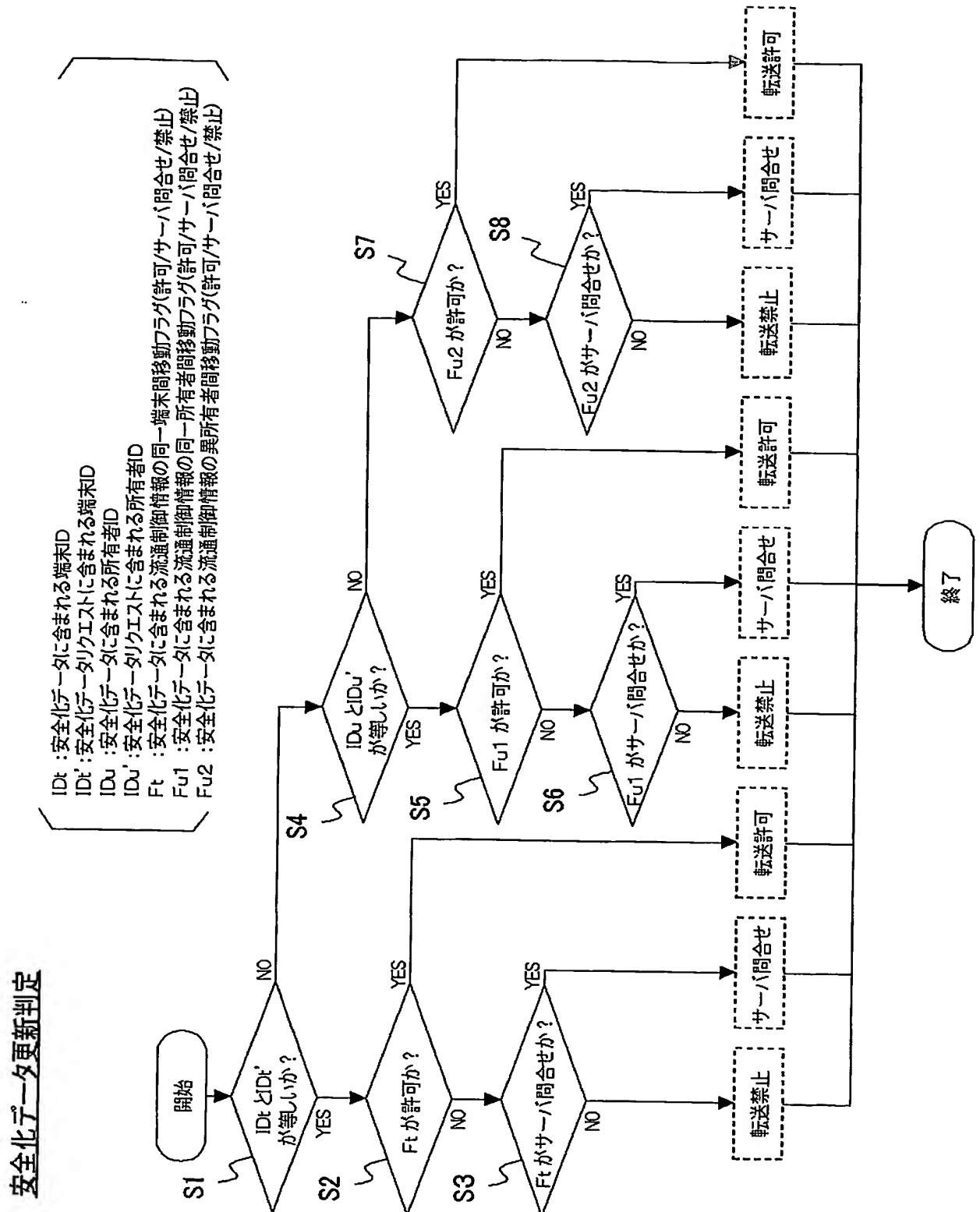


Fig.10

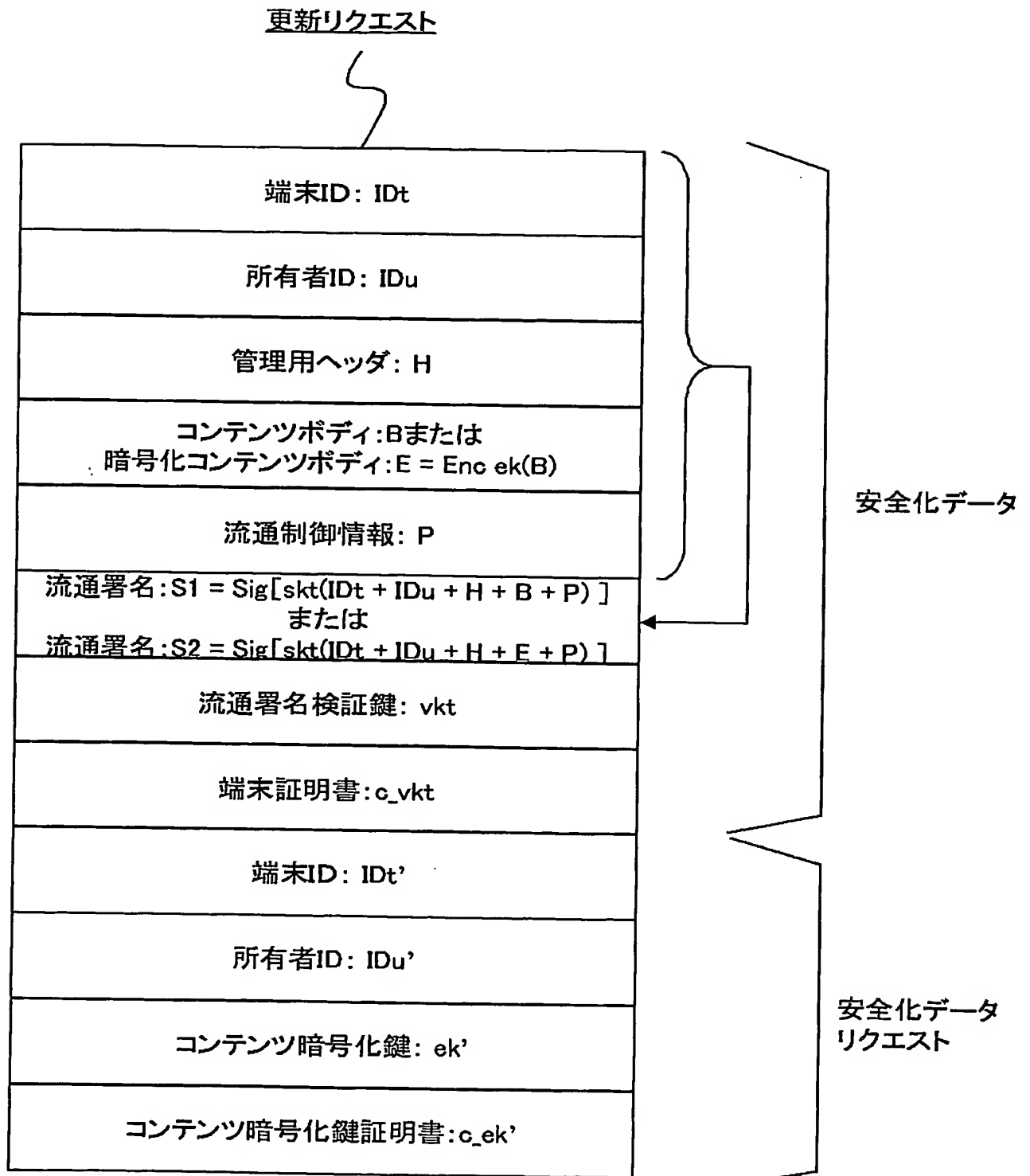
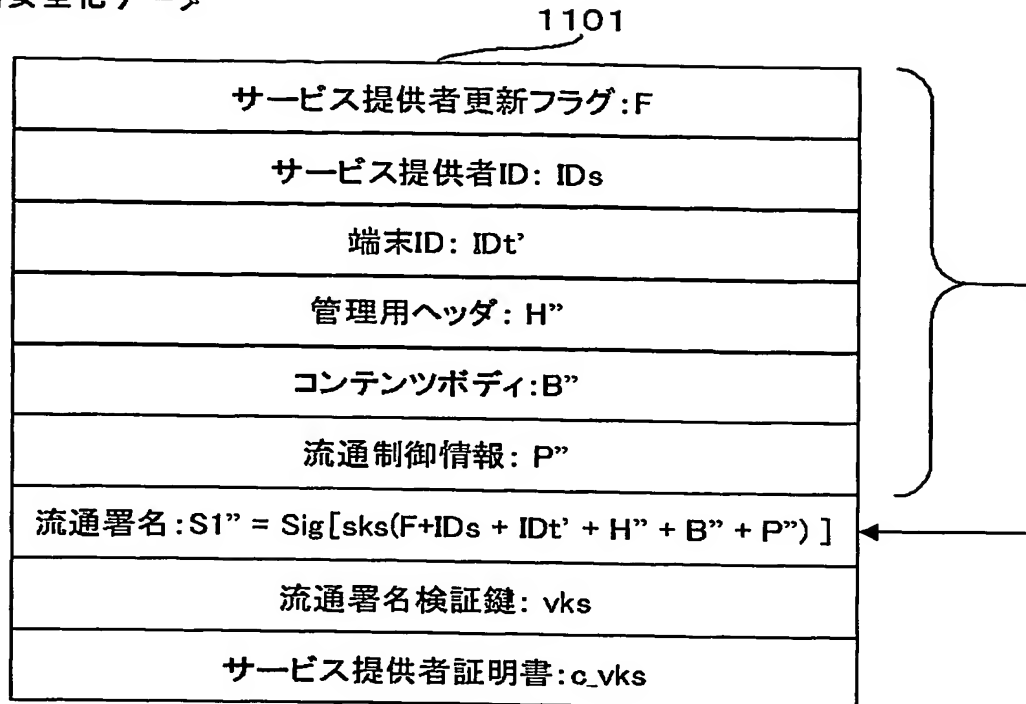




Fig.11

## (A) 更新安全化データ



## (B) 暗号化指定の更新安全化データ

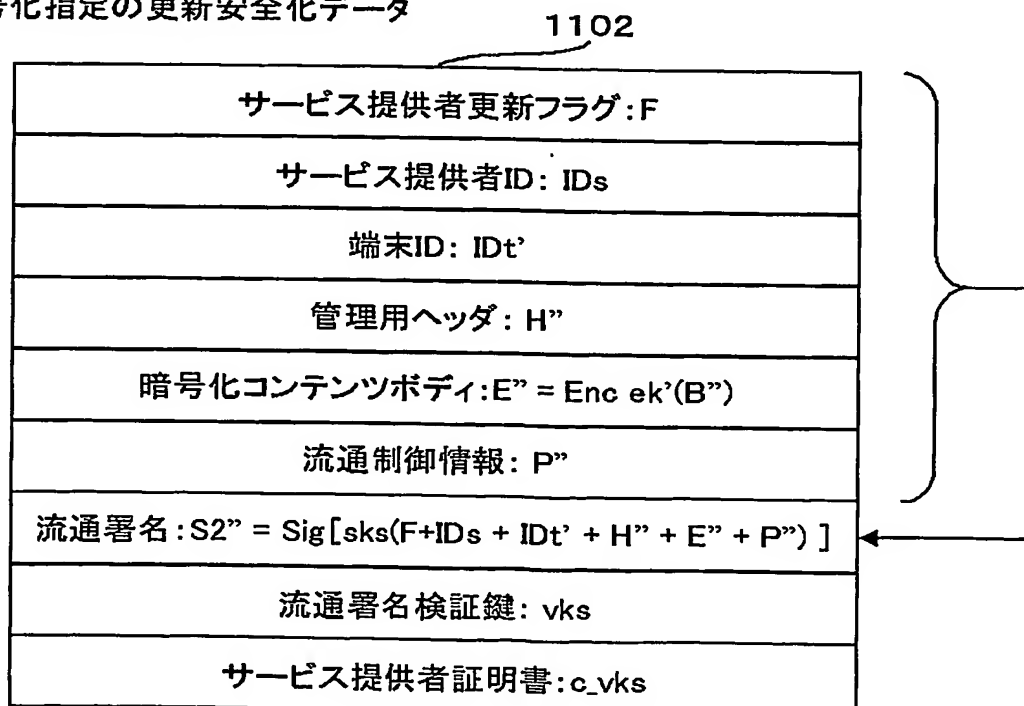


Fig.12

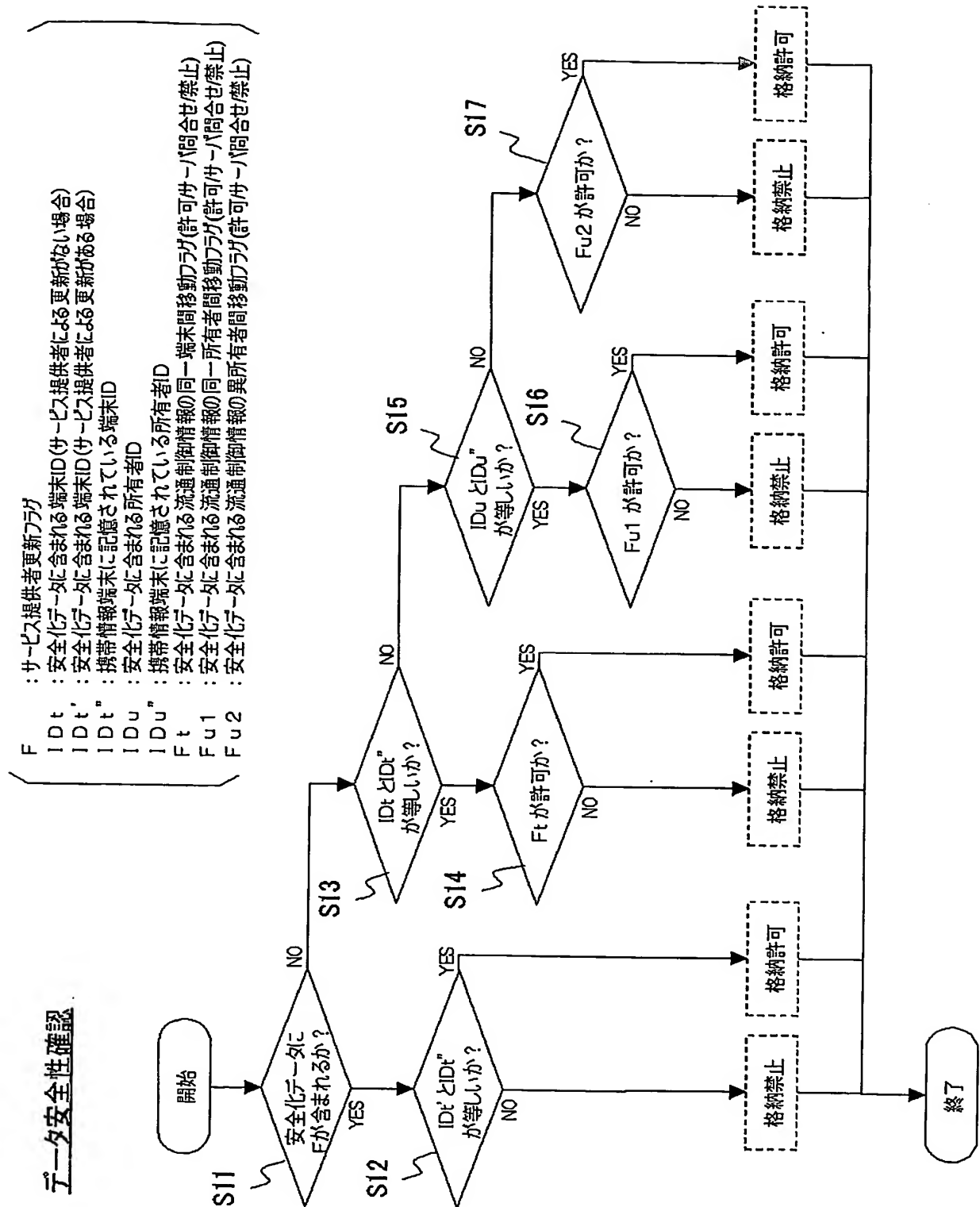




Fig.14

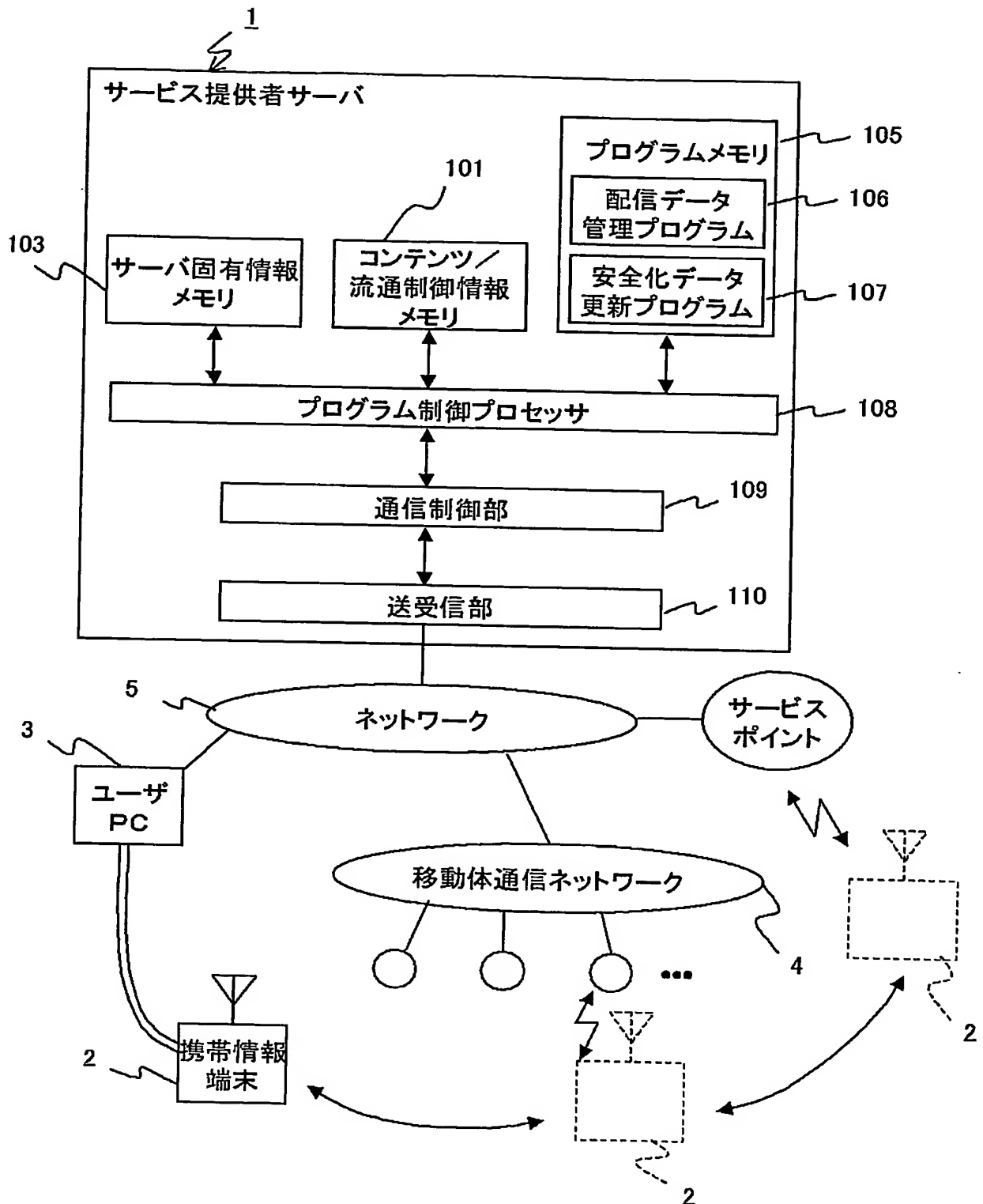


Fig.15

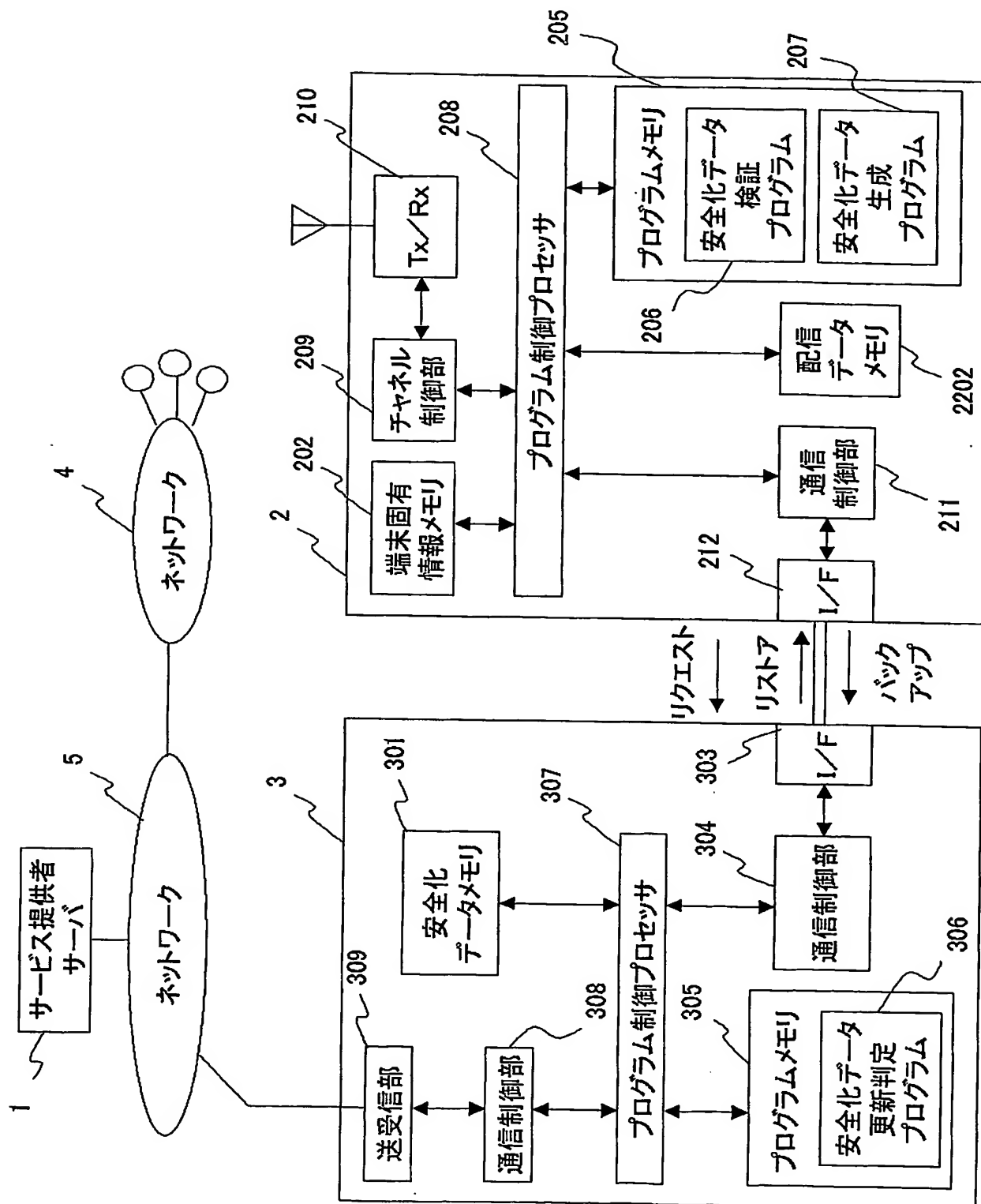


Fig.16

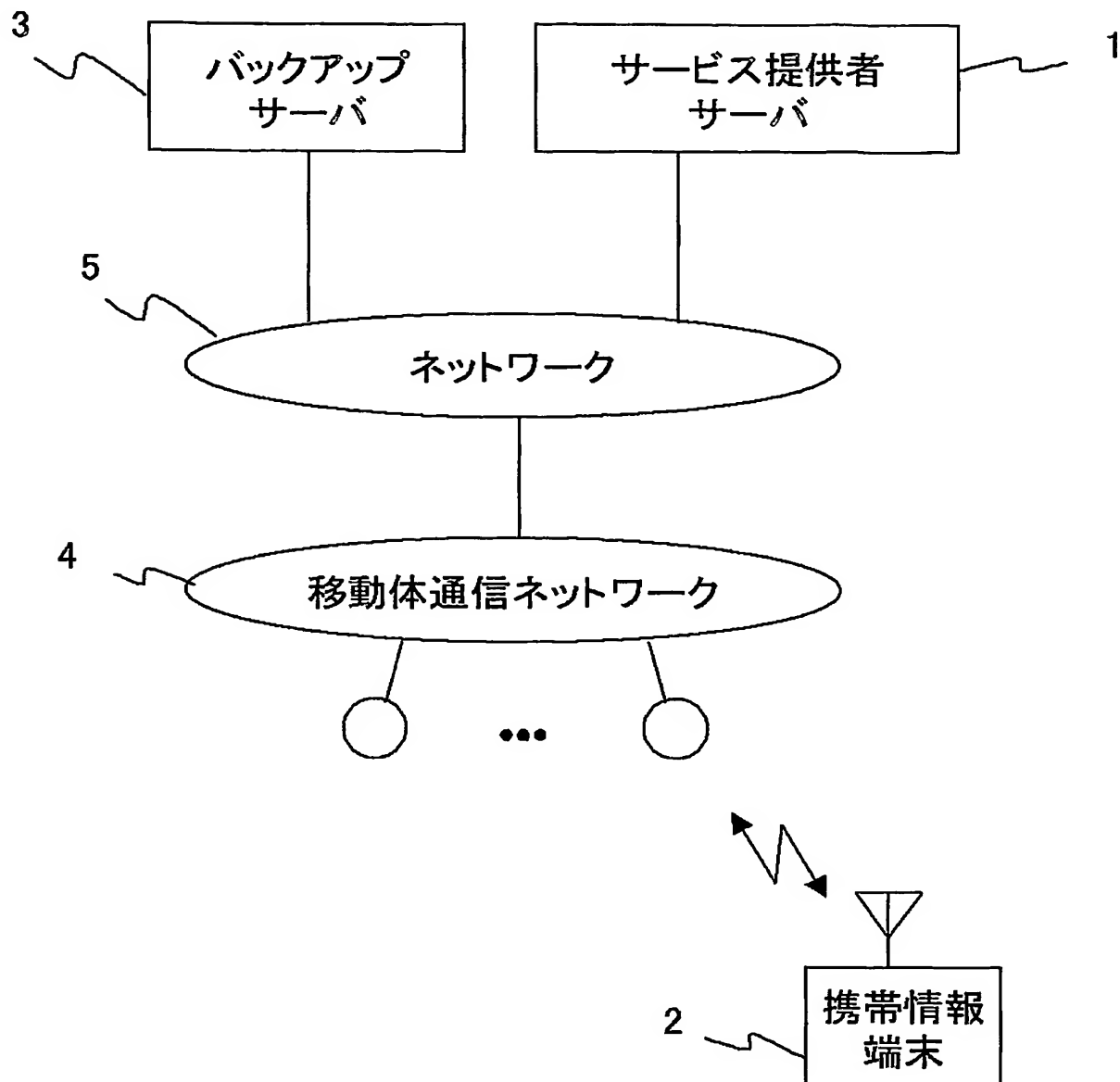


Fig.17

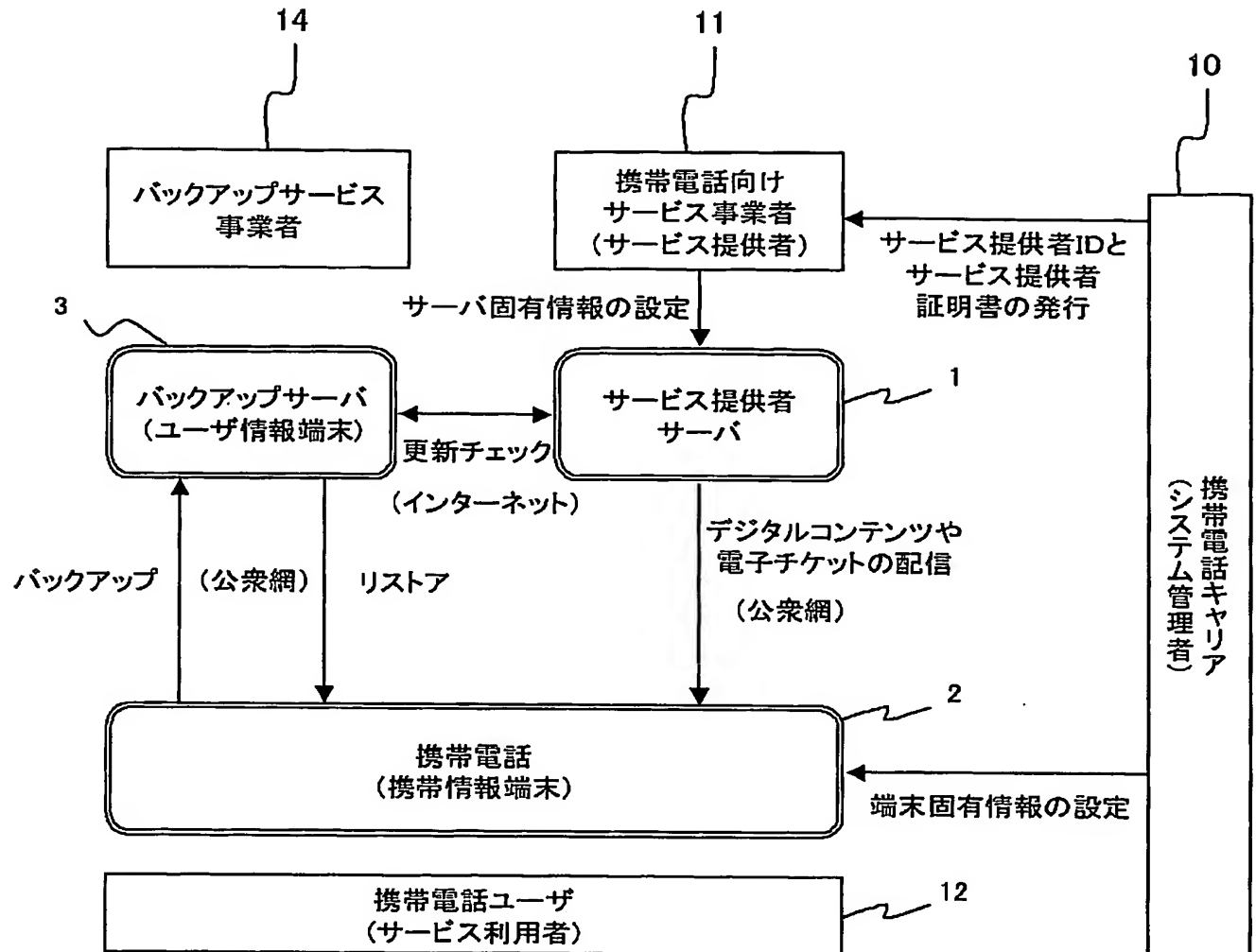


Fig.18

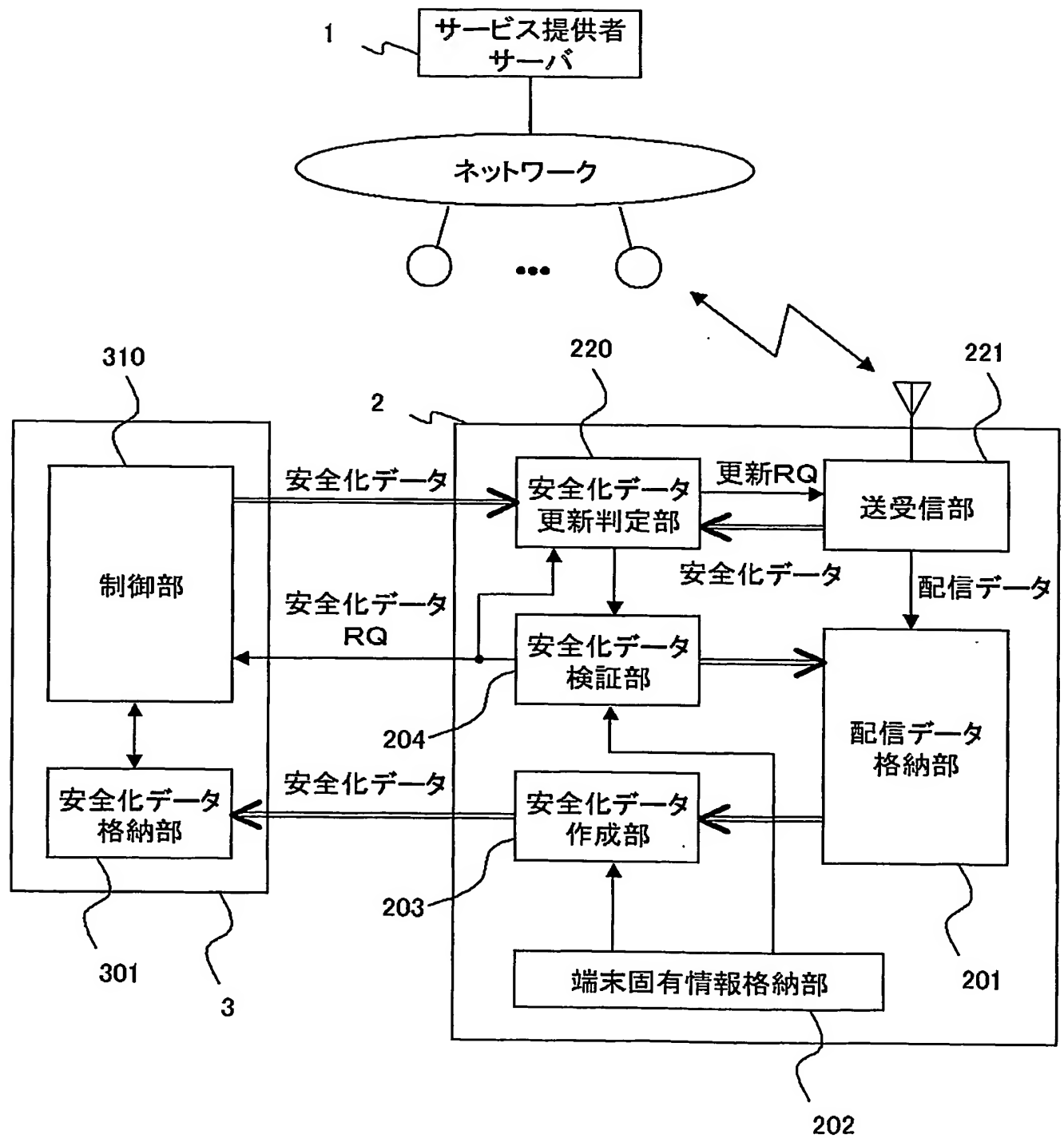




Fig.19

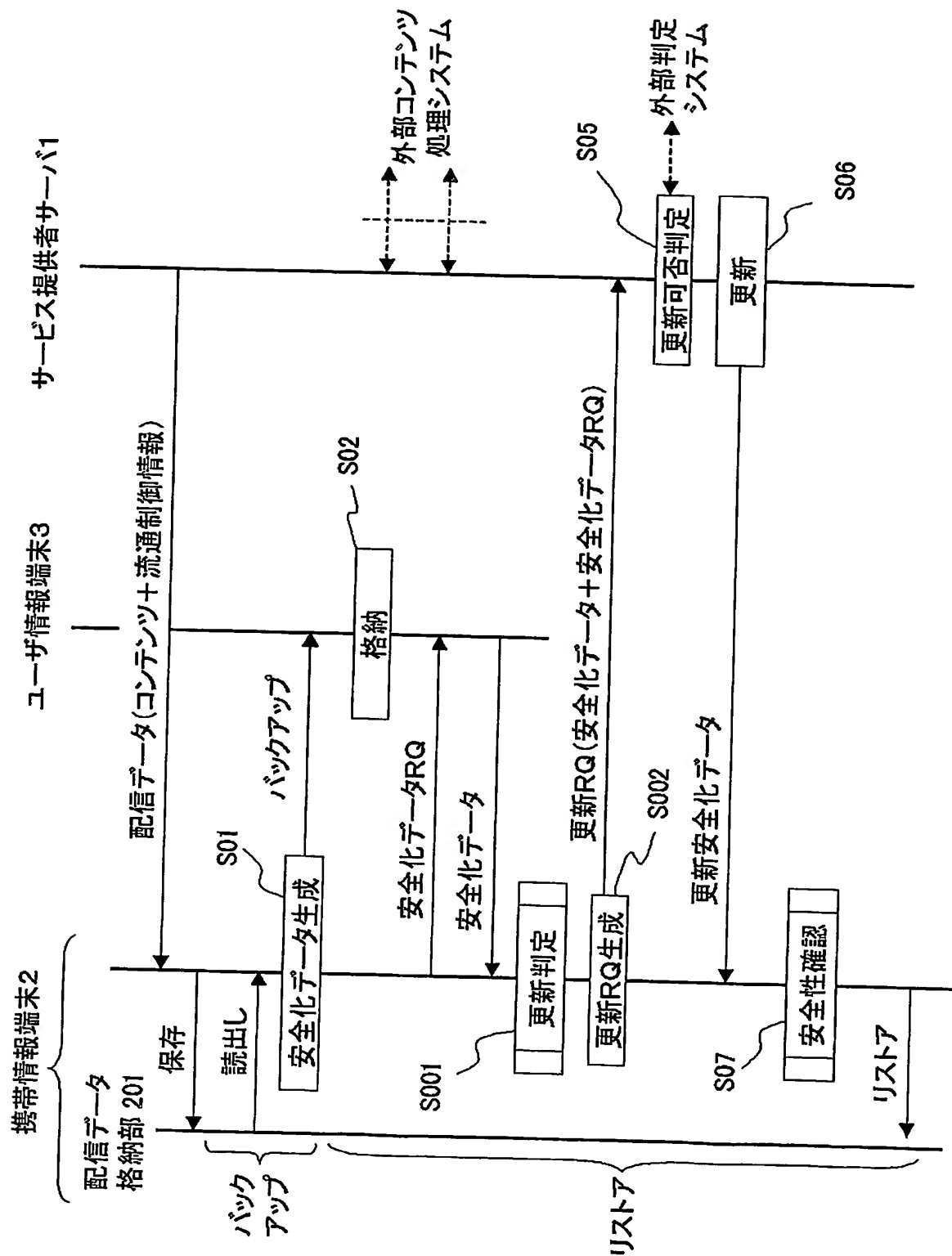


Fig.20

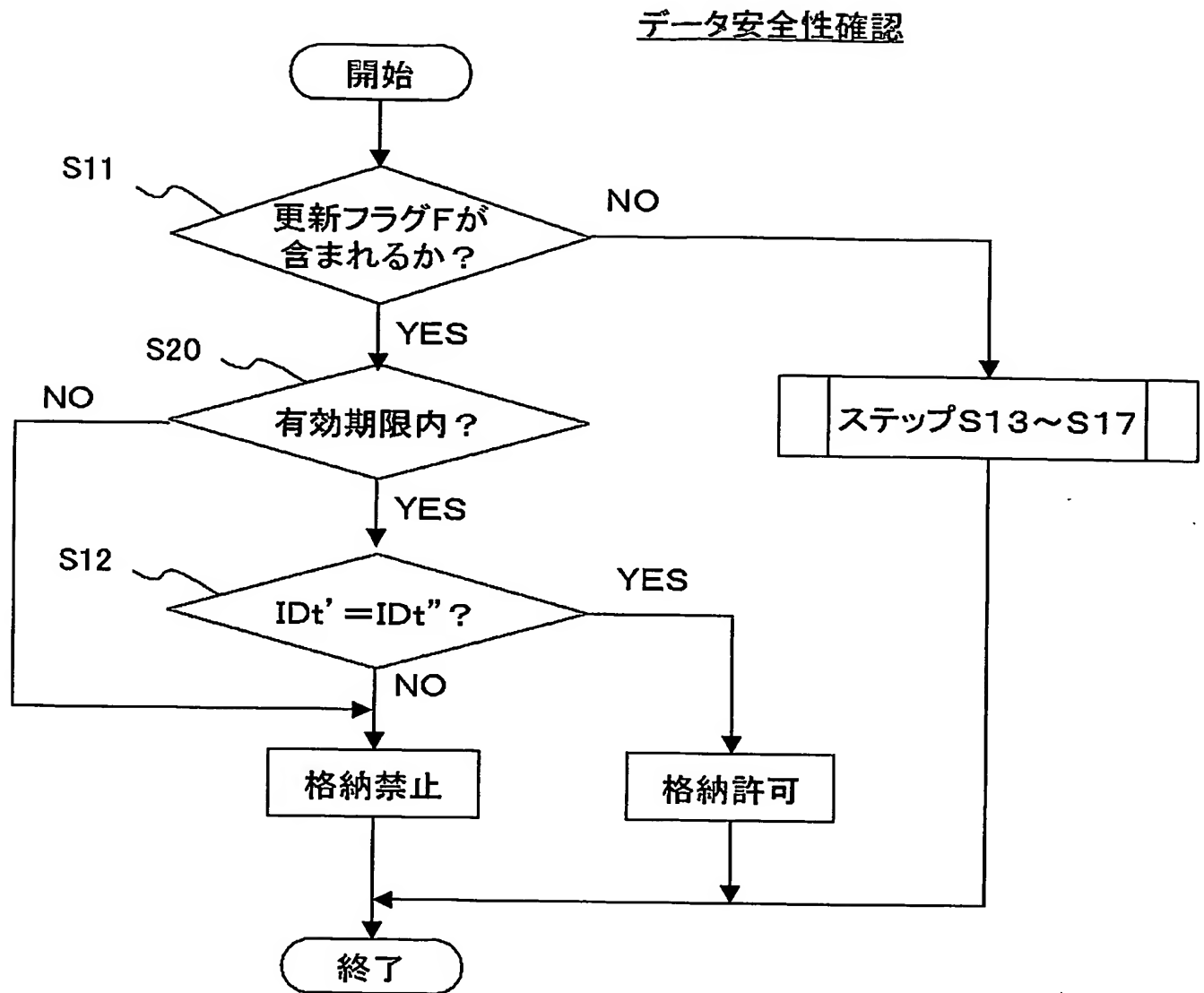


Fig.21

## 安全化データリクエスト



端末ID: $ID_t'$
所有者ID: $ID_u'$
コンテンツ暗号化鍵: $ek'$
コンテンツ暗号化鍵証明書: $c_{ek}'$
乱数 $r$

Fig.22

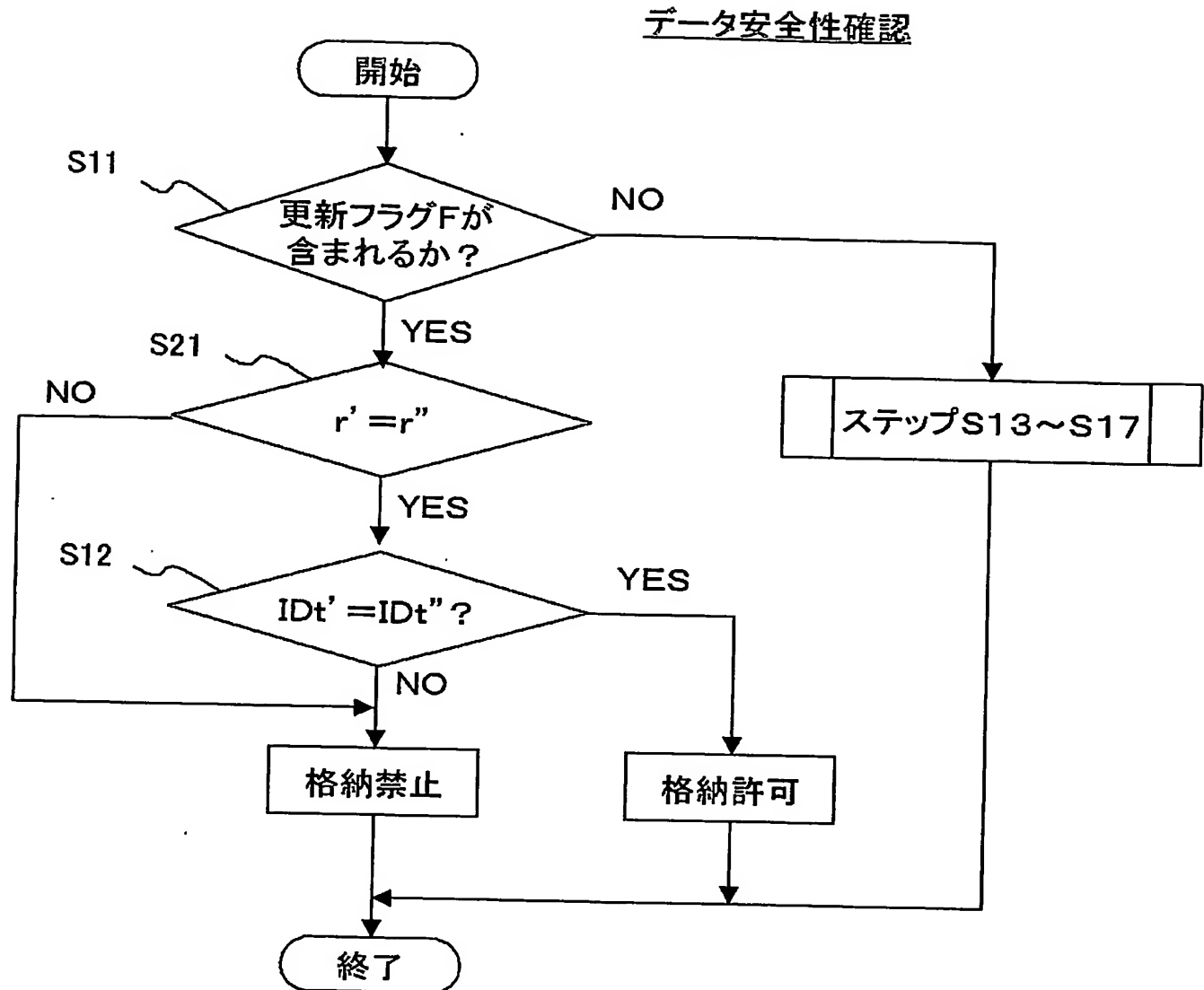


Fig.23

```
enum RESULT {restoreDirect, restoreAfterServerUpdate, restoreFobiedden};

RESULT Check(          int terminal_id1,          int terminal_id2,
                   int user_id1,          int user_id2,          )
{
    //端末IDが一致する場合はリストア許可
    if (terminal_id1 == terminal_id2)
        return restoreDirect;

    //リストア日が2004年2月14日で、userIDが一致している場合は、
    //サーバ問い合わせ後リストア許可
    char currentDate[9];
    _strdate(currentDate);
    if (strcmp (currentDate, "02/14/04") == 0 && user_id1 == user_id2 )
        return restoreAfterServerUpdate;

    //リストア不許可
    return restoreFobidden;
}
```

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006042

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F12/14, 15/00, 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14, 15/00, 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT.

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2003-58430 A (Sony Corp.), 28 February, 2003 (28.02.03), Par. Nos. [0059] to [0126]; all drawings (Family: none)	1, 4 2, 3, 5-24
X A	JP 2003-85048 A (Sony Corp.), 20 March, 2003 (20.03.03), Par. Nos. [0442] to [0477]; Figs. 49 to 52 (Family: none)	19-22 1-18, 23-24
A	JP 2002-342168 A (J-Phone Higashi Nihon Kabushiki Kaisha), 29 November, 2002 (29.11.02), Full text; all drawings (Family: none)	1-24

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
02 June, 2004 (02.06.04)Date of mailing of the international search report  
22 June, 2004 (22.06.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006042

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-99074 A (Casio Computer Co., Ltd.), 04 April, 2003 (04.04.03), Full text; all drawings (Family: none)	1-24
A	JP 2003-22338 A (Matsushita Electric Industrial Co., Ltd.), 24 January, 2003 (24.01.03), Full text; all drawings & WO 2003/005207 A1	1-24
A	JP 2002-351744 A (Sony Corp.), 06 December, 2002 (06.12.02), Full text; all drawings (Family: none)	1-24
A	JP 2002-63076 A (Nippon Telegraph And Telephone Corp.), 28 February, 2002 (28.02.02), Full text; all drawings (Family: none)	1-24

A. 発明の属する分野の分類 (国際特許分類 (IPC))  
Int. Cl<sup>7</sup>. G06F12/14, 15/00, 17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))  
Int. Cl<sup>7</sup>. G06F12/14, 15/00, 17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2004年  
日本国登録実用新案公報 1994-2004年  
日本国実用新案登録公報 1996-2004年

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X A	JP 2003-58430 A (ソニー株式会社) 2003. 02. 28, 段落【0059】 - 【0126】, 全図 (ファミリーなし)	1, 4 2, 3, 5-24
X A	JP 2003-85048 A (ソニー株式会社) 2003. 03. 20, 段落【0442】 - 【0477】; 第49-52図 (ファミリーなし)	19-22 1-18, 23-24
A	JP 2002-342168 A (ジェイフォン東日本株式会社) 2002. 11. 29, 全文, 全図 (ファミリーなし)	1-24

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

02. 06. 2004

国際調査報告の発送日

22. 6. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

相崎 裕恒

5 N

9 2 9 0

電話番号 03-3581-1101 内線 3585



C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2003-99074 A (カシオ計算機株式会社) 2003. 04. 04, 全文, 全図 (ファミリーなし)	1-24
A	JP 2003-22338 A (松下電器産業株式会社) 2003. 01. 24, 全文, 全図 & WO 2003/005207 A1	1-24
A	JP 2002-351744 A (ソニー株式会社) 2002. 12. 06, 全文, 全図 (ファ ミリーなし)	1-24
A	JP 2002-63076 A (日本電信電話株式会社) 2002. 02. 28, 全文, 全図 (ファミリーなし)	1-24